Forensic Falcon™ User's Manual

Logicube, Inc.

Chatsworth, CA 91311

USA

Phone: 818 700 8488

Fax: 818 700 8466

Version: 2.4.2

Date: 07/24/15

MAN-FALCON

Limitation of Liability and Warranty Information

Logicube Disclaimer

LOGICUBE IS NOT LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO PROPERTY DAMAGE, LOSS OF TIME OR DATA FROM USE OF A LOGICUBE PRODUCT, OR ANY OTHER DAMAGES RESULTING FROM PRODUCT MALFUNCTION OR FAILURE OF (INCLUDING WITHOUT LIMITATION, THOSE RESULTING FROM: (1) RELIANCE ON THE MATERIALS PRESENTED, (2) COSTS OF REPLACEMENT GOODS, (3) LOSS OF USE, DATA OR PROFITS, (4) DELAYS OR BUSINESS INTERRUPTIONS, (5) AND ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE (OR FROM DELAYS IN SERVICING OR INABILITY TO RENDER SERVICE ON ANY) LOGICUBE PRODUCT.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ALL PRODUCTS. HOWEVER, THE CUSTOMER IS RESPONSIBLE TO VERIFY THAT THE OUTPUT OF LOGICUBE PRODUCT MEETS THE CUSTOMER’S QUALITY REQUIREMENT. THE CUSTOMER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCT AND/OR SOFTWARE, OR HARDWARE PROBLEMS, CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY CUSTOMER, EITHER UNDER WARRANTY OR ON A TIME AND MATERIALS BASIS.

Warranty

DISCLAIMER

IMPORTANT - PLEASE READ THE TERMS OF THIS AGREEMENT CAREFULLY. BY INSTALLING OR USING LOGICUBE PRODUCTS, YOU AGREE TO BE BOUND BY THIS AGREEMENT.

IN NO EVENT WILL LOGICUBE BE LIABLE (WHETHER UNDER THIS AGREEMENT, RESULTING FROM THE PERFORMANCE OR USE OF LOGICUBE PRODUCTS, OR OTHERWISE) FOR ANY AMOUNTS REPRESENTING LOSS OF PROFITS, LOSS OR INACCURACY OF DATA, LOSS OR DELAYS OF BUSINESS, LOSS OF TIME, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, SERVICES, OR TECHNOLOGY, PROPERTY DAMAGE, OR INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF A PURCHASER OR USER OF LOGICUBE PRODUCTS OR ANY THIRD PARTY. LOGICUBE’S AGGREGATE LIABILITY IN CONTRACT, TORT, OR OTHERWISE (WHETHER UNDER THIS AGREEMENT, RESULTING FROM THE PERFORMANCE OR USE OF LOGICUBE PRODUCTS, OR OTHERWISE) TO A PURCHASER OR USER OF LOGICUBE PRODUCTS SHALL BE LIMITED TO THE AMOUNT PAID BY THE PURCHASER FOR THE LOGICUBE PRODUCT. THIS LIMITATION OF LIABILITY WILL BE EFFECTIVE EVEN IF LOGICUBE HAS BEEN ADVISED OF THE POSSIBILITY OF ANY SUCH DAMAGES.

LOGICUBE MAKES EVERY EFFORT TO ENSURE PROPER OPERATION OF ITS PRODUCTS. HOWEVER, THE PURCHASER IS RESPONSIBLE FOR VERIFYING THAT THE OUTPUT OF A LOGICUBE PRODUCT MEETS THE

PURCHASER’S REQUIREMENTS. THE PURCHASER FURTHER ACKNOWLEDGES THAT IMPROPER OPERATION OF LOGICUBE PRODUCTS CAN CAUSE LOSS OF DATA, DEFECTIVE FORMATTING, OR DEFECTIVE DATA LOADING. LOGICUBE WILL MAKE EFFORTS TO SOLVE OR REPAIR ANY PROBLEMS IDENTIFIED BY PURCHASER, EITHER UNDER THE WARRANTY SET FORTH BELOW OR ON A TIME AND MATERIALS BASIS.

LIMITED WARRANTY

FOR ONE YEAR FROM THE DATE OF SALE (THE “WARRANTY PERIOD”) LOGICUBE WARRANTS THAT THE PRODUCT (EXCLUDING CABLES, ADAPTERS, AND OTHER “CONSUMABLE” ITEMS) IS FREE FROM MANUFACTURING DEFECTS IN MATERIAL AND WORKMANSHIP. THIS LIMITED WARRANTY COVERS DEFECTS ENCOUNTERED IN THE NORMAL USE OF THE PRODUCT DURING THE WARRANTY PERIOD AND DOES NOT APPLY TO: PRODUCTS DAMAGED DUE TO PHYSICAL ABUSE, MISHANDLING, ACCIDENT, NEGLIGENCE, OR FAILURE TO FOLLOW ALL OPERATING INSTRUCTIONS CONTAINED IN THE OPERATING MANUAL; PRODUCTS WHICH ARE MODIFIED; PRODUCTS WHICH ARE USED IN ANY MANNER OTHER THAN THE MANNER FOR WHICH THEY WERE INTENDED, AS SET FORTH IN THE OPERATING MANUAL; PRODUCTS WHICH ARE DAMAGED OR DEFECTS CAUSED BY THE USE OF UNAUTHORIZED PARTS OR BY UNAUTHORIZED SERVICE; PRODUCTS DAMAGED DUE TO UNSUITABLE OPERATING OR PHYSICAL CONDITIONS DIFFERING FROM THOSE RECOMMENDED IN THE OPERATING MANUAL OR PRODUCT SPECIFICATIONS PROVIDED BY LOGICUBE; ANY PRODUCT WHICH HAS HAD ANY OF ITS SERIAL NUMBERS ALTERED OR REMOVED; OR ANY PRODUCT DAMAGED DUE TO IMPROPER PACKAGING OF THE WARRANTY RETURN TO LOGICUBE. AT LOGICUBE’S OPTION, ANY PRODUCT PROVEN TO BE DEFECTIVE WITHIN THE WARRANTY PERIOD WILL EITHER BE REPAIRED OR REPLACED USING NEW OR REFURBISHED COMPONENTS AT NO COST. THIS WARRANTY IS THE SOLE AND EXCLUSIVE REMEDY FOR DEFECTIVE PRODUCTS. IF A PRODUCT IS HAS BECOME OBSOLETE OR IS NO LONGER SUPPORTED BY LOGICUBE THE PRODUCT MAY BE REPLACED WITH AN EQUIVALENT OR SUCCESSOR PRODUCT AT LOGICUBE’S DISCRETION. THIS WARRANTY EXTENDS ONLY TO THE END PURCHASER OF LOGICUBE PRODUCTS. THIS WARRANTY DOES NOT APPLY TO, AND IS NOT FOR THE BENEFIT OF, RESELLERS OR DISTRIBUTORS OF LOGICUBE PRODUCTS. UNLESS OTHERWISE AGREED IN WRITING BY LOGICUBE, NO WARRANTY IS PROVIDED TO RESELLERS OR DISTRIBUTORS OF LOGICUBE PRODUCTS.
IN ORDER TO RECEIVE WARRANTY SERVICES CONTACT LOGICUBE’S TECHNICAL SUPPORT DEPARTMENT VIA PHONE OR E-MAIL. PRODUCTS RETURNED TO LOGICUBE FOR REPAIR UNDER WARRANTY MUST REFERENCE A LOGICUBE RETURN MATERIAL AUTHORIZATION NUMBER (“RMA”). ANY PRODUCT RECEIVED BY LOGICUBE WITHOUT AN RMA# WILL BE REFUSED AND RETURNED TO PURCHASER. THE PURCHASER MUST CONTACT LOGICUBE’S TECHNICAL SUPPORT DEPARTMENT VIA E-MAIL (SUPPORT@LOGICUBE.COM) OR VIA PHONE AT +1-818-700-8488 OPT. 3 TO OBTAIN A VALID RMA#. THE PURCHASER MAY BE REQUIRED TO PERFORM CERTAIN DIAGNOSTIC TESTS ON A PRODUCT PRIOR TO LOGICUBE ISSUING AN RMA#. THE PURCHASER MUST PROVIDE THE PRODUCT MODEL, SERIAL NUMBER, PURCHASER NAME AND ADDRESS, EMAIL ADDRESS AND A DESCRIPTION OF THE PROBLEM WITH AS MUCH DETAIL AS POSSIBLE. AT LOGICUBE’S SOLE AND ABSOLUTE DISCRETION, REASONABLE TELEPHONE AND EMAIL SUPPORT MAY ALSO BE AVAILABLE FOR THE LIFE OF THE PRODUCT AS DEFINED BY LOGICUBE.

EXCEPT AS OTHERWISE SPECIFICALLY PROVIDED IN THIS AGREEMENT, LOGICUBE PRODUCTS ARE PROVIDED AS-IS AND AS-AVAILABLE, AND LOGICUBE DISCLAIMS ANY AND ALL OTHER WARRANTIES (WHETHER EXPRESS, IMPLIED, OR STATUTORY) INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT OF THIRD PARTY RIGHTS.
SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

RoHS Certificate of Compliance

LOGICUBE PRODUCTS COMPLY WITH THE EUROPEAN UNION RESTRICTION OF THE USE OF CERTAIN HAZARDOUS SUBSTANCES IN ELECTRONIC EQUIPMENT, ROHS DIRECTIVE (2002/95/EC).

THE ROHS DIRECTIVE PROHIBITS THE SALE OF CERTAIN ELECTRONIC EQUIPMENT CONTAINING SOME HAZARDOUS SUBSTANCES SUCH AS MERCURY, LEAD, CADMIUM, HEXAVALENT CHROMIUM AND CERTAIN FLAME-RETARDANTS IN THE EUROPEAN UNION. THIS DIRECTIVE APPLIES TO ELECTRONIC PRODUCTS PLACED ON THE EU MARKET AFTER JULY 1, 2006.

Logicube Technical Support Contact Information

1. By website: www.logicube.com
2. By email: techsupport@logicube.com
3. By telephone: 1 - (818) 700 8488 ext. 3 between the hours of 7am – 5pm PST, Monday through Friday, excluding U.S. legal holidays.

Table of Contents

1: Introduction

1.0 Introduction to the Logicube Falcon

Welcome to the Logicube Forensic Falcon™. Falcon sets a new standard in digital forensic imaging. Without exception, the fastest and most technologically advanced forensic imaging solution available. Feature-packed, power-rich performance in a space-saving footprint that provides expandability to meet future technology advances. This unparalleled solution is designed for demanding forensic imaging tasks and sets a new standard of excellence in digital forensic data imaging solutions.

1.1 Features

- The Falcon is the fastest forensic imaging solution available, achieving speeds of 23GB/min* and meets future hard drive speed improvements with SAS/SATA-3 6GB/s maximum rated speed of 37GB/min.
- **Image and verify to the following formats**: native copy, dd image, e01, ex01 and file-based copy. Compression available for E01/Ex01 formats. Uses SHA1, SHA256, or MD5 authentication.
- **4 Source and 5 Destination ports.** Write-protected source ports include 2 SAS/SATA, 1 USB 3.0, and 1 FireWire. Destination ports include 2 SAS/SATA, 2 USB 3.0, and 1 FireWire. A Gigabit Ethernet port for network connectivity is also available. USB source and destination can be converted to SATA using a USB to SATA converter.
- Built in support for SAS/SATA/USB/FireWire storage devices. Adapters are included with Falcon to support 1.8”/2.5”/3.5” IDE and 1.8” ZIF and microSATA drive interfaces. Optional adapter are available for eSATA, mSATA, and CompactFlash drives. An optional SCSI module provides support for 1 SCSI source and 1 Destination drive.

- **Image to or from a network location.** Use the falcon to image to a network location using CIFS protocol and/or image from a network location using iSCSI. Users can use iSCSI as a source or destination drive.
- **Network services.** Users can disable various network services (such as HTTP, SSH, Telnet, CIFS/NETBIOS, iSCSI, Iperf, and Ping) for security purposes.
- **Preview/triage hard drive contents.** Preview the drive contents directly on the Falcon. The file browser feature provides logical access to source or destination drives connected to Falcon. Users can view the drive's partitions and contents, and view text files, jpeg, PDF, XML, HTML files. Other file types (such as .doc and .xls) can be viewed by connecting Falcon to a network and via a PC, download and view. The Falcon also allows you to preview suspect/source drives or destination drives using the USB connection from the Falcon to a computer, or by using the SMB protocol. Users can also use the iSCSI protocol to preview Source drives.
- Use a **web browser** to manage all operations remotely. Easily connect to a networked Falcon from your laptop or desktop using a web browser. The interface features automatic page scaling for iPad type devices.
- **Image from a desktop or laptop PC** without removing the hard drive. Create a forensic bootable USB flash drive that allows the user to image a source drive from a computer on the same network without booting the computer's native operating system.
- **Image from a Mac®.** Image from a Mac® system booted in "target disk mode" using the write-blocked FireWire port on falcon. The Mac's internal drive is seen as a source drive. Macs with either FireWire or Thunderbolt ports can be connected to the Falcon. A Thunderbolt to FireWire adapter is required.
- **Multi-task.** Shorten the evidence collection process with the ability to wipe one destination drive while imaging to another, or image from multiple source drives to multiple destinations. Perform up to five tasks concurrently.
- **Parallel Imaging.** Perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. Clone to a network location or a destination drive in mirror copy format while simultaneously imaging in e01 or dd format to a different destination drive.
- **Concurrent Image+Verify** (patent-pending). The Falcon takes advantage of destination drives that are faster than the source drive and begins verification while the imaging process is occurring. Duration of total image plus verification process time may be reduced by up to half.
- The Falcon can perform a **forensic, filter-based file copy**. Filter and then image specific file types by file extension such as .PDF, .doc, .jpeg, .mov, etc.
- Secure sensitive evidence data with whole drive **AES 256 bit Encryption**. Decryption can be performed using the Falcon or by using open source software programs such as FreeOTFE or TrueCrypt.
- **Fast Multi-pass wipe** (DoD specifications) or use secure erase to wipe drives, wipe at speeds of up to 27GB/min.
- **The Network Push feature** allows the user to push evidence files from destination drives connected to the Falcon or from a Falcon repository, to a network location. A more secure method than simply copying and pasting to the analysis computer, the Falcon performs an MD5 or SHA hash during the push process, a log file is generated for each push process.

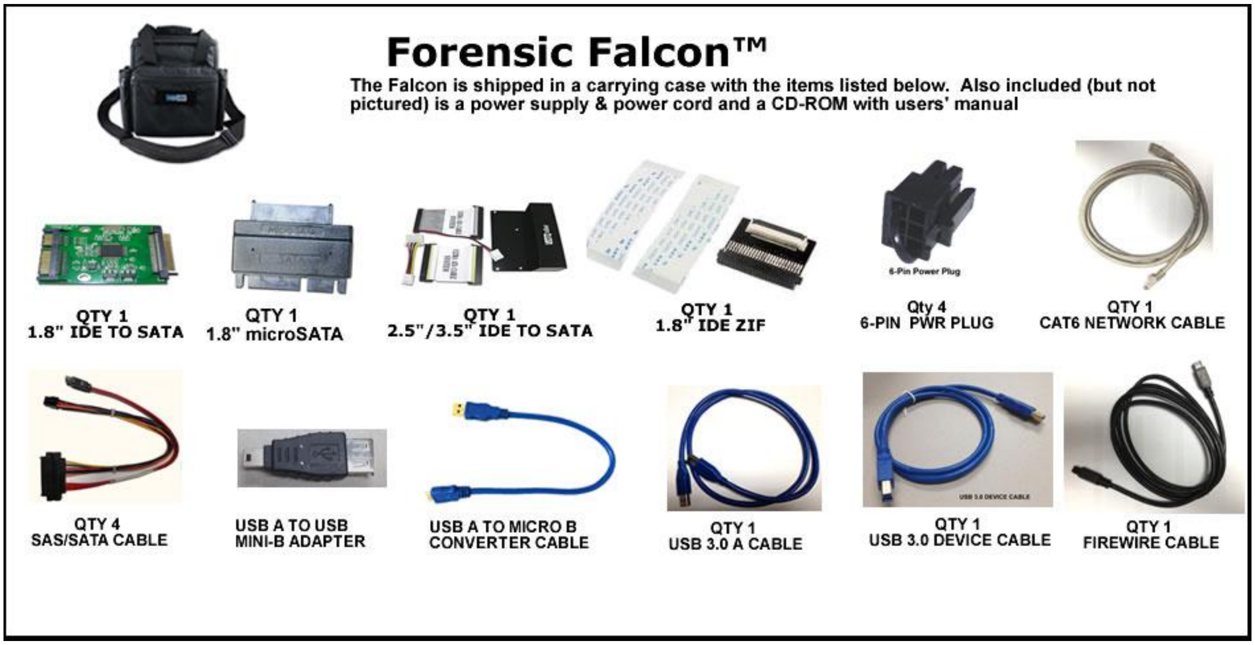
- **Image to an external storage device** (such as a NAS) using the Gigabit Ethernet, USB 3.0, or SAS/SATA connection.
- **Task Macro feature.** Set specific tasks to be performed sequentially, for example, first wipe the destination drive then hash the source drive then image the source drive. Set-up your Macro, press start and all tasks within the Macro will be performed automatically.
- Features an **internal, removable storage drive** that stores OS and audit trail/logs. The drive is easily removed for secure/classified locations.
- **Audit Trail/Log files** provide detailed information on each operation. Log files can be viewed on Falcon or via a web browser, exported to XML, HTML, or PDF format to a USB enclosure. Users can print the log files directly from their PC when connected to Falcon via a web browser.
- **Additional features** include HPA/DCO capture, drive "trim" feature to manipulate the DCO and HPA areas of destination drives, the ability to set password-protected user profiles and save configurations, drive "time-out" feature automatically puts drives in stand-by mode after a specified idle time, drive spanning, large 7" color touch screen display, on-screen keyboard, two USB 2.0 host ports for keyboard, mouse or printer connectivity, and an HDMI port to connect a projector or monitor.

*The falcon achieves 23GB/min imaging speed using solid state drives in native copy and in e01/Ex01 image format. Your results may vary depending on the specification and condition of the hard drive used as well as the mode, image format and settings used during the imaging process.

1.2 In the Box

The complete Falcon system includes the following:

- The Logicube Falcon unit
- AC adapter/Power supply and power cable
- 1 CAT6 Network cable
- 4 SAS/SATA cables
- 1 USB 3.0 type A cable
- 1 USB 3.0 device cable
- 1 USB A Female to USB Mini-B 5 Pin Male adapter
- 1 USB 3.0 A Female to Micro B Male (USB 3.0) cable
- 1.8" microSATA adapter
- 1.8" IDE ZIF to SATA adapter
- 2.5"/3.5" IDE to SATA adapter
- 1.8" IDE to SATA adapter
- 4 6-Pin Power plugs
- 1 FireWire cable
- CD-ROM containing the user's manual
- Carrying case



Forensic Falcon™

The Falcon is shipped in a carrying case with the items listed below. Also included (but not pictured) is a power supply & power cord and a CD-ROM with users' manual

1.3 Options

The following options are available for the Forensic Falcon:

- SCSI Module provides 1 write-protected source port and 1 destination port. Built-in support for 68-pin SCSI drives
- 50-pin SCSI adapter for use with SCSI Module
- 80-pin SCSI adapter for use with SCSI Module
- eSATA cable
- mSATA adapter
- Flash Media Reader for compact flash cards,
- SD cards and other flash media
- USB 3.0 to SATA Adapter
- USB 3.0 4-port Hub

1.4 Specifications

Power Requirements	Power Consumption	Operating Temperature	Relative Humidity	Net Weight	Dimensions	Agency Approvals
12 VDC 12 Amp	< 140W with drives	0 to 40°C (32 to 104°F)	20% to 80%	2.4lbs/1.09k 9lbs/4.3k with case & shipping box	8.5" W X 3" H X6.25" D 21.6cm X 7.6cm X15.9cm	RoHs compliant FCC Part 15 Class A CE

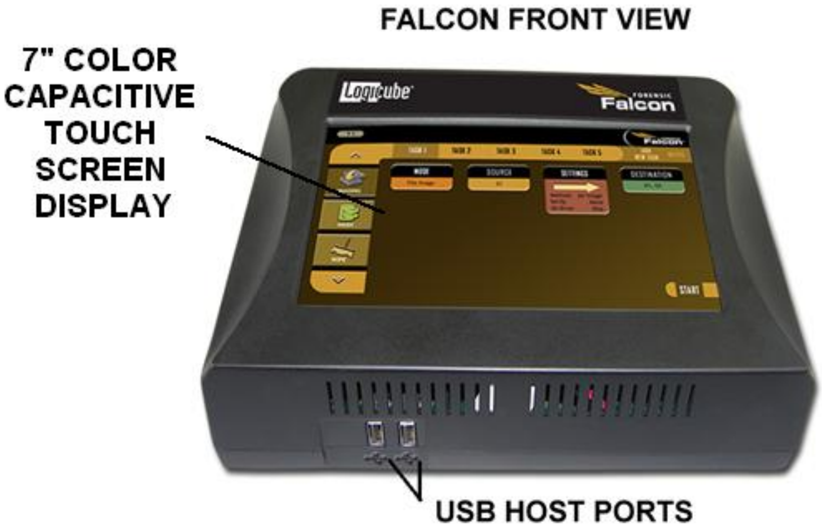
⚠ **WARNINGS:** ⚠

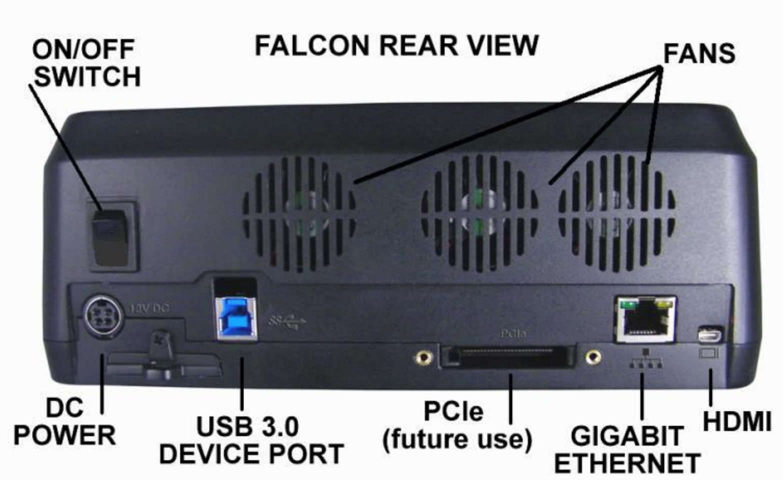
- Never connect a suspect drive to the Destination ports of the Forensic Falcon as data may be overwritten.
- Incorrectly connecting the suspect drive to the system can result in data on the suspect drive to be lost forever.
- Avoid dropping the Logicube Forensic Falcon or subjecting it to sharp jolts. When in use, place it on a flat surface.
- Keep the unit dry. If the Forensic Falcon needs to be cleaned, use a lightly damp, lint free cloth. Avoid using soap or other cleaning agents particularly those containing bleach, ammonia, alcohol or other harsh chemicals.
- Do not attempt to service or open the Logicube Forensic Falcon. Doing so may void the warranty. If the unit requires service, please contact Logicube Technical Support for assistance.

2: Getting Started

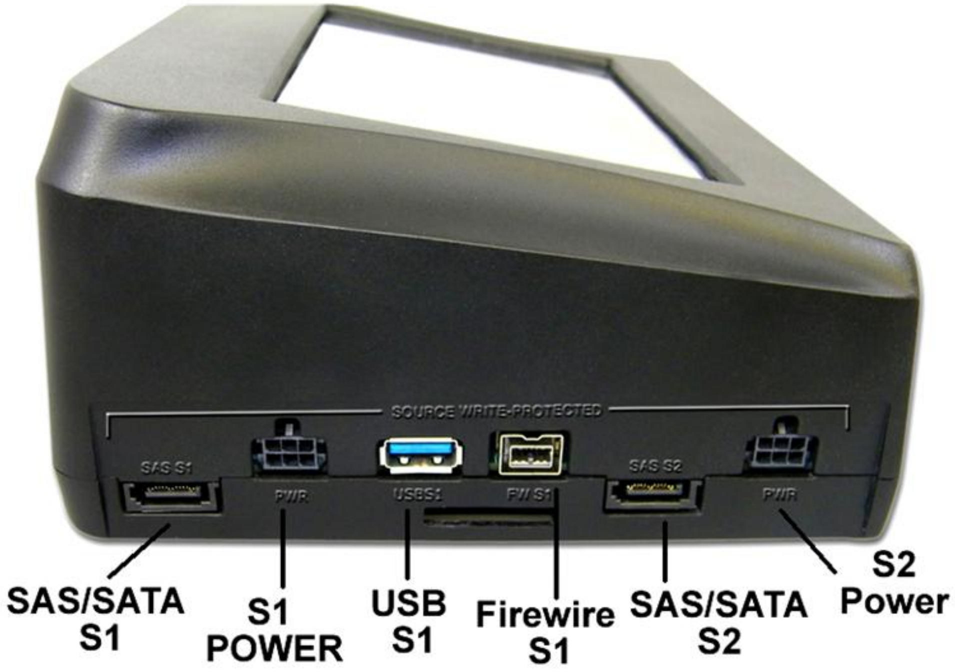
2.0 Overview of the Falcon

Special Icons – Throughout this manual, there are two icons that can be seen. Please pay close attention when any of these two icons are found. These icons highlight additional information or important warnings on specific topics.

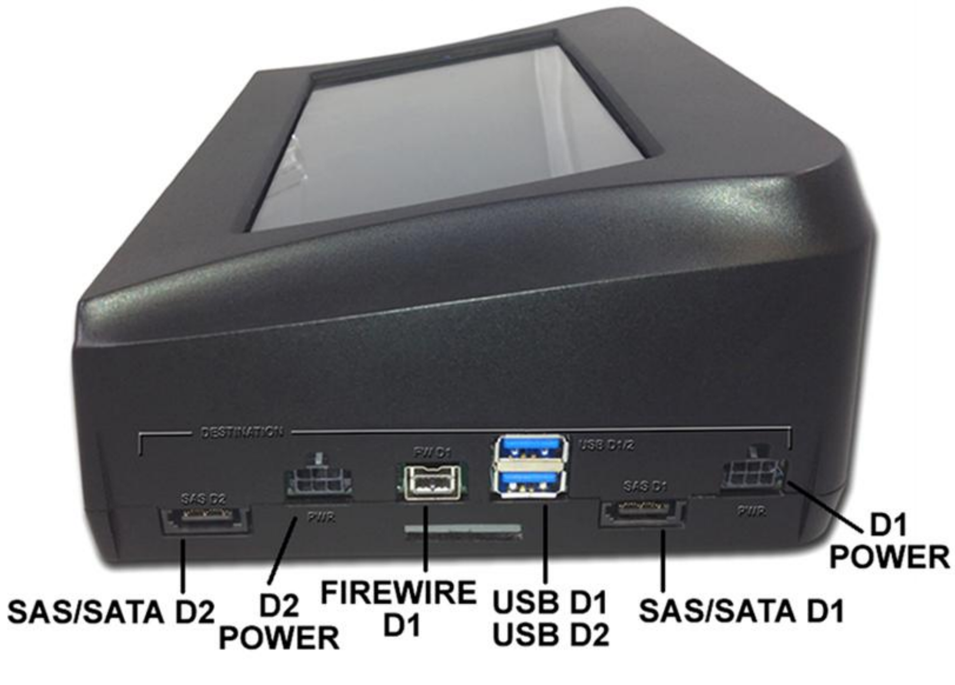




FALCON LEFT SIDE VIEW
SOURCE WRITE-PROTECTED PORTS



FALCON RIGHT SIDE VIEW
DESTINATION PORTS



2.1 Turning the Falcon on and off

The Falcon comes with a 12V, 12.5A (output DC) power supply that connects to the back of the device. Attach the included power supply to the Falcon's DC power port in the back.

To turn the Falcon on, press and immediately release the top of the momentary on/off switch in the back. The Falcon will turn on and start the boot process.

It is normal for the fans to either turn off or slow down after the initial start-up sequence.

There are two ways of turning the Falcon off:

1. Press and immediately release the top of the momentary on/off switch in the back. The Falcon will begin its shut down process and after a few seconds, the display and fans will turn off.
2. Using the Graphical User Interface (GUI) either on the touch screen or via a browser through a remote connection, navigate to the ***Power Off*** screen and tap or click the ***Power Off*** icon.

2.2 Connecting various drive types

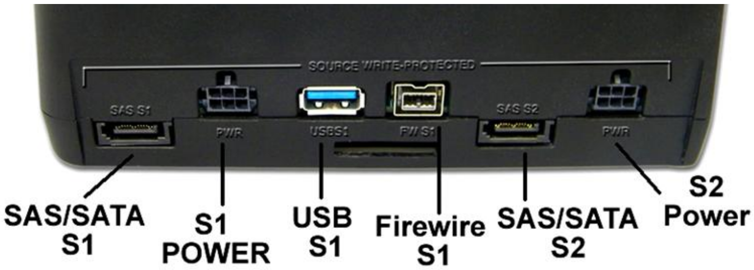
Cables and adapters are available for the following drive types:

- SAS
- SATA
- USB
- FireWire
- 1.8" microSATA
- 2.5" and 3.5" PATA/IDE
- 1.8" ZIF
- 1.8" PATA/IDE
- eSATA (optional)
- mSATA (optional)
- Flash Media (optional)

2.2.1 Connecting Source Drives

Source drives (also called suspect drives) must be connected to the left side of the Falcon. These ports are write-protected and are labeled as follows:

- SAS S1 – SAS/SATA data port for the Source 1 (S1) position.
- SAS S2 – SAS/SATA data port for the Source 2 (S2) position.
- PWR – power port for either Source 1 (S1) or Source 2 (S2) position.
- USBS1 – USB 3.0 Source port
- FW S1 – FireWire Source port



Source drives do not have to be connected in any order. For example, a single SATA Source drive does not have to be connected to the SAS/SATA S1 port. It can be connected to the SAS/SATA S2 port without having anything connected to the S1 port.

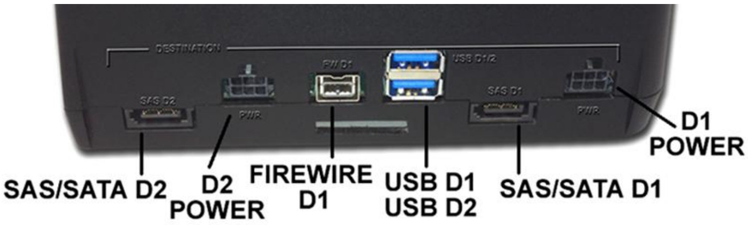
Never connect a suspect or Source drive to the Destination ports of the Falcon. Data may be overwritten if a drive is connected to a Destination port.

Any combination of drives can be connected, up to 4 Source drives. For example, one SAS drive, one SATA drive, one USB drive, and one FireWire drive can all be connected at the same time.

2.2.2 Connecting Destination Drives

Destination drives (also called evidence drives) must be connected to the right side of the Falcon. These ports are labeled as follows:

- SAS D1 – SAS/SATA data port for the Destination 1 (D1) position.
- SAS D2 – SAS/SATA data port for the Destination 2 (D2) position.
- PWR – power port for either Destination 1 (D1) or Destination 2 (D2) position.
- USB D1/2 – USB 3.0 Destination port
- FW D1 – FireWire Destination port



Destination drives do not have to be connected in order. For example, a single SATA Destination drive does not have to be connected to the SAS/SATA D1 port. It can be connected to the SAS/SATA D2 port without having anything connected to the D1 port.

Any combination of drives can be connected, up to 5 Destination drives. For example, one SAS drive, one SATA drive, two USB drives, and one FireWire drive can all be connected at the same time.

The Falcon ports are hot swappable. Drives that are not being used in any task (image, hash, wipe, etc.) can be disconnected any time.

Some drives are not hot swappable. Please check with the drive manufacturer to find out if the drive being used does not support hot swapping.

When disconnecting drives, it is very important to make sure the drives are not being used on any task. Disconnecting drives while the Falcon is using the drive for a task may cause data loss.

2.2.3 Connecting USB 3.0 Drives

USB 3.0 is a new technology and USB 3.0 controller manufacturers may have variations in device designs that have inconsistent adherence to USB 3.0 specification. This may result in non-detection of the USB 3.0 device on certain equipment (including desktops, laptops or the Falcon). If a USB 3.0 device cannot be detected on the Falcon USB ports we have found that using a USB 3.0 hub may stabilize and regulate the communication between the USB 3.0 device and the Falcon, allowing the device to be detected properly. We have identified and qualified a USB 3.0 hub which is available as an option. For more information on the USB 3.0 hub, please see **Section 12.5**.

2.2.4 Using USB/FireWire/eSATA enclosures

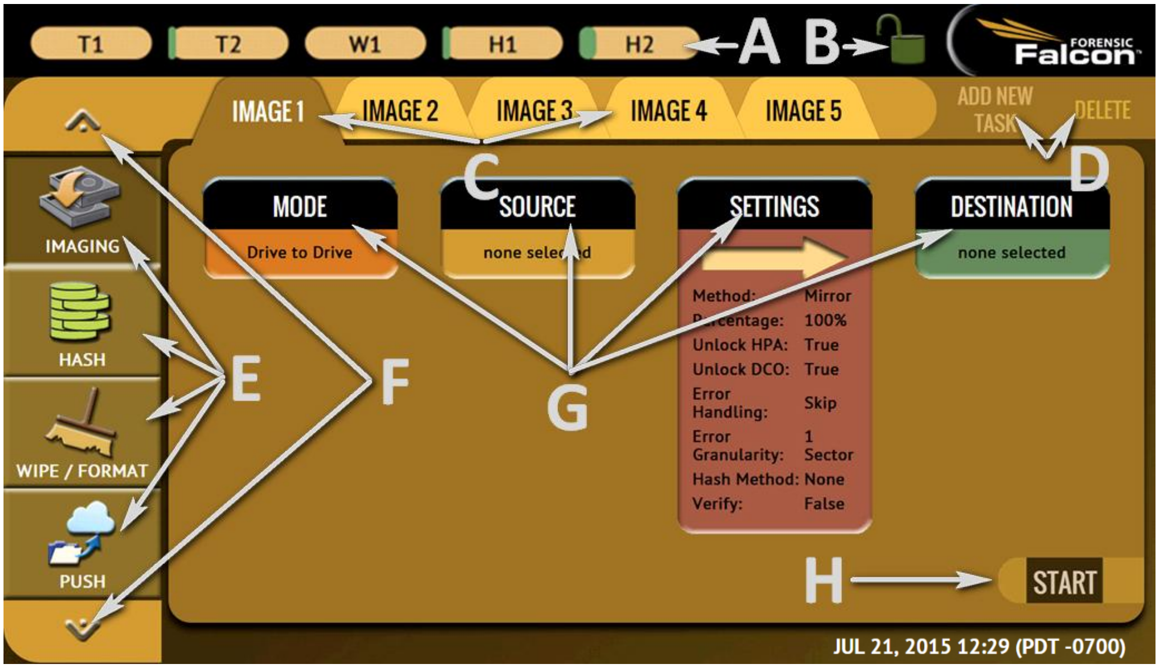
When using USB, FireWire, and/or eSATA enclosures, it is highly recommended to leave the drive inside the enclosure. USB enclosures typically have an on-board controller that may be necessary to read the drive properly. Taking the drive out of the enclosure could cause any device (including computers) not to read the drive contents properly.

2.2.5 Connecting SATA Drives using a USB-to-SATA adapter

Logicube has qualified a USB 3.0 to SATA adapter for use with the Falcon. This adapter provides the capability to connect SATA drives to the USB 3.0 ports on the Falcon and uses a USB 3.0 to SATA converter. USB 3.0 is a new technology and USB 3.0 controller manufacturers may have variations in device designs that have inconsistent adherence to USB 3.0 specifications. This adapter and other USB 3.0 enclosures may experience communication disruption between devices. If the adapter is not detected properly we have found that using a USB 3.0 hub may stabilize and regulate the communication between the Adapter or USB 3.0 enclosure, and the Falcon, allowing the device to be detected properly. We have identified and qualified a USB 3.0 hub which is available as an option. For more information on the USB 3.0 to SATA adapter, please see **Section 12.4**. For more information on the USB 3.0 hub, please see **Section 12.5**.

2.3 The user interface

The user interface (UI) has been designed to quickly and easily input commands. It is simple and intuitive showing common icons such as tasks, modes of operation, and scroll icons on the screen. The UI is designed to be easily followed, going from left to right across the screen.



MODE: Drive to Drive

SOURCE: none selected

DESTINATION: none selected

Method:	Mirror
Percentage:	100%
Unlock HPA:	True
Unlock DCO:	True
Error Handling:	Skip
Error Granularity:	1 Sector
Hash Method:	None
Verify:	False

JUL 21, 2015 12:29 (PDT -0700)

A – Operations/Tasks currently running (displays up to 5 total tasks)
B – Lock indicator/shortcut
C – Operations/Tasks
D – Add or delete tasks
E – Types of Operations
F – Up and down scroll arrows
G – Operations options and settings
H – Start icon

2.4 Touch screen

The Falcon features a 7" color LCD capacitive touch screen that allows the user to quickly input commands. The screen is bright and easy to read.

2.5 HDMI

The Falcon has an HDMI port located in the back panel. Simply connect an HDMI cable from the Falcon to an external display that supports HDMI and Falcon will automatically show the display on both the Falcon and the external display.

To change the display resolution on the external display:

1. Connect a wired USB keyboard to one of the front USB host ports.
2. Press ALT+R. An on-screen display should appear on the external display that allows the display resolution to be changed.

3: Quick Start

3.0 Quick Start Guide

This chapter gives a basic overview and steps on how to perform different types of operations using the Falcon (Image, Hash, Wipe, etc.). Complete details on each operation, menu, or selection, and the different screens can be found in **Chapter 5: Imaging** and **Chapter 6: Types of Operation**.

The Falcon can perform up to five (5) tasks per mode of operation (specifically Image, Hash, and/or Wipe).

3.1 Imaging

This type of operation allows the imaging of a Source drive to one or more Destinations. There are three (3) different imaging modes and several settings to choose from. These selections should be performed in order from left to right.

- **Drive to Drive** – Performs a bit-for-bit copy of the Source producing an exact duplicate of the Source drive. This is also known as a native copy or mirror copy.
- **Drive to File** – Images the Source to any of the following image output file formats: ***DD***, ***E01***, or ***EX01***. Compression is available for E01 and EX01 formats.

E01 and EX01 files created on the Destination may be smaller than the selected ***Segment Size*** if compression is used. For example, if 4GB segment size selected, some files may be less than 4GB. This occurs when there is a lot of blank space on the Source drive.

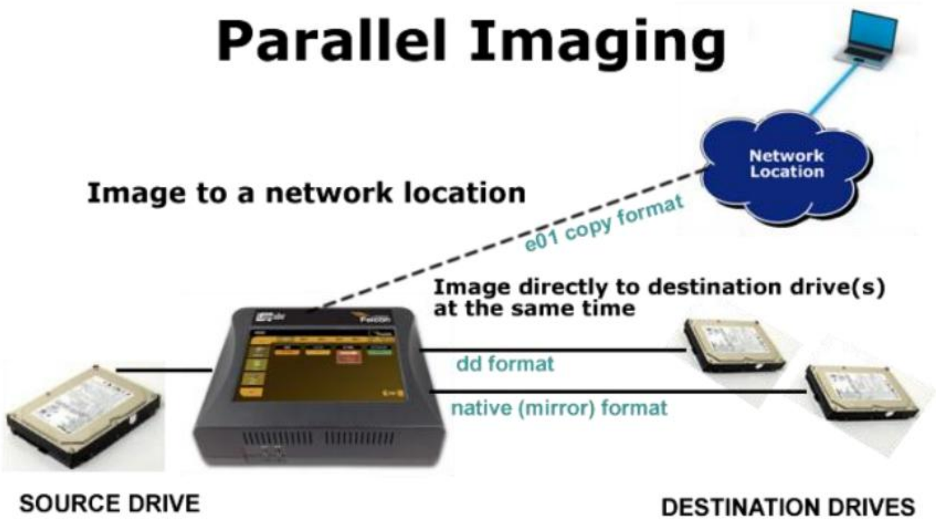
- **File to File** – Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source. If a hash method is selected, each file will be hashed.

Details on the different screens found in the Imaging operation can be found in **Chapter 5: Imaging.**

Definition: Source/Destination/Repository – A Source, Destination, or Repository can be a drive (Hard Disk Drive, Solid State Drive, USB drive, etc.), Flash media (SD card, CF card, etc.), or network location.

Falcon uses a concurrent Image+Verify process (Patent pending). When ***Verify*** is set, the Falcon images and verifies concurrently and takes advantage of destination hard drives that may be faster than the source hard drive. Duration of total image process time may be reduced by up to half.

Falcon can also perform Parallel Imaging. A user can simultaneously perform multiple imaging tasks from the same source drive to multiple destinations using different imaging formats. For example, image to a network location or a destination drive using the E01 format while imaging to a different destination drive using native/mirror or DD format.

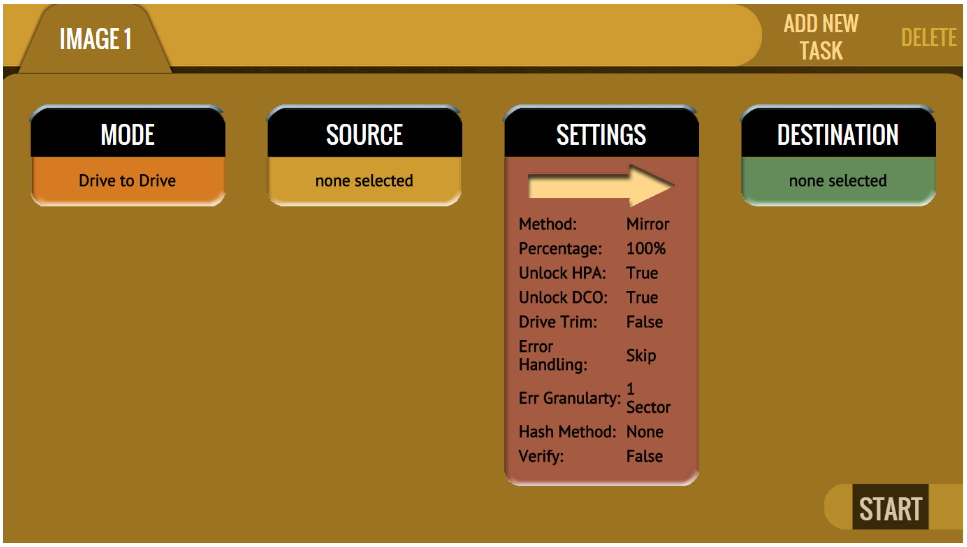


The Falcon imaging, hash, and wipe speeds are determined by several factors including the following:

- The manufacturer specifications of the drive(s) being used
- The age of the drive (manufactured date)
- How often that drive has been used

For example, a 2 TB drive with 64MB of cache produced by the manufacturer 2 years ago is most likely slower than a 2 TB drive that the same manufacturer just released this year, even though they are both 7200RPM with 64MB of cache, and are both SATA III.

3.1.1 Step-by-step instructions – Imaging



MODE	Drive to Drive
SOURCE	none selected
DESTINATION	none selected

Method:	Mirror
Percentage:	100%
Unlock HPA:	True
Unlock DCO:	True
Drive Trim:	False
Error Handling:	Skip
Err Granularity:	1 Sector
Hash Method:	None
Verify:	False

Details on each selectable option on the Image screen can be found in ***Section 5.0 Imaging***.

1. Select ***Imaging*** from the types of operation on the left side.
2. Tap the ***Mode*** icon and select ***Drive to Drive***, ***Drive to File***, or ***File to File*** then tap the ***OK*** icon.
3. Tap the ***Source*** icon and choose the source from the list of connected drives then tap the ***OK*** icon.
4. Tap the ***Settings*** icon and adjust the settings as needed (***Case Info***, ***File Image Method Settings or Mirror Settings***, ***HPA/DCO***, ***Error Handling***, ***Hash/Verification Method***, ***etc.***) then tap the ***OK*** icon.

- The Settings screen will be different for each of the three modes. Details on the different Settings screens can be found in **Chapter 5: Imaging**.
- Log file names can be set in ***Settings*** in the ***Case Info*** screen by entering a Case/File name. See **Section 5.0.3.1** for more information.

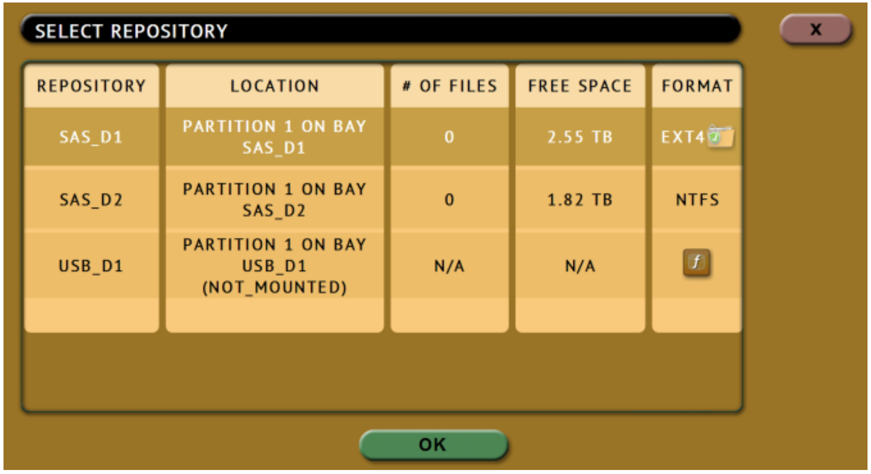
The Falcon will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores “_“ when creating the log or file names.

POSIX portable characters are:

Uppercase A to Z
Lowercase a to z
Numbers 0 to 9

Period (.)
Underscore (_)
Hyphen/Dash (-)

5. Tap the ***Destination*** icon and select the destination(s) to be used then tap the ***OK*** icon.



SELECT REPOSITORY

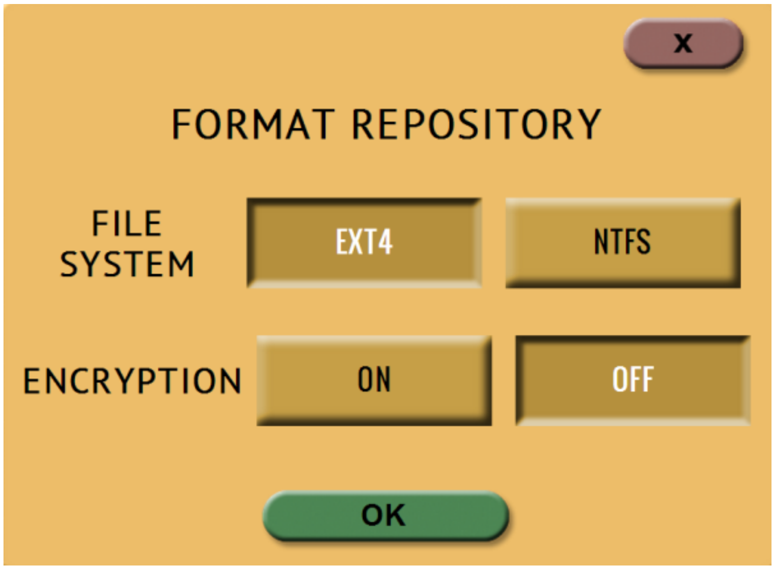
REPOSITORY	LOCATION	# OF FILES	FREE SPACE	FORMAT
SAS_D1	PARTITION 1 ON BAY SAS_D1	0	2.55 TB	EXT4 📁
SAS_D2	PARTITION 1 ON BAY SAS_D2	0	1.82 TB	NTFS
USB_D1	PARTITION 1 ON BAY USB_D1 (NOT_MOUNTED)	N/A	N/A	ƒ

For DD, E01, Ex01, and File to File mode, the Falcon uses the NT file system (NTFS) or EXT4 file systems to format drives. If the Destination drive is not formatted properly, the ***Location*** will appear as "***(NOT_MOUNTED)***" and a format icon will appear in the Format column. Tap the ƒ ***(Format)*** icon the Destination drive.

For Drive to File or File to File, the Falcon will display drives connected to the Destination ports and any added repository.

Encrypted drives will have the following symbol in the Format column: 📁

When formatting the drive from this screen, a prompt will appear to format the drive.



FORMAT REPOSITORY

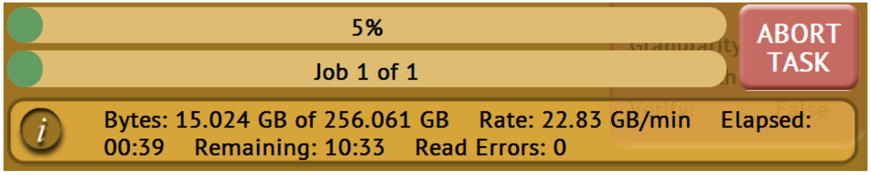
FILE SYSTEM [✓ EXT4] NTFS

ENCRYPTION ON [✓ OFF]

Select which file system to use (EXT4 or NTFS) and whether to format with encryption (ON) or without encryption (OFF). Details on encryption can be found in Chapter 8 of the Falcon User's Manual. For details on formatting a drive, see ***Section 6.0.3.2.3***. Formatting the drive may take up to two minutes. Tap the ***OK*** icon to continue.

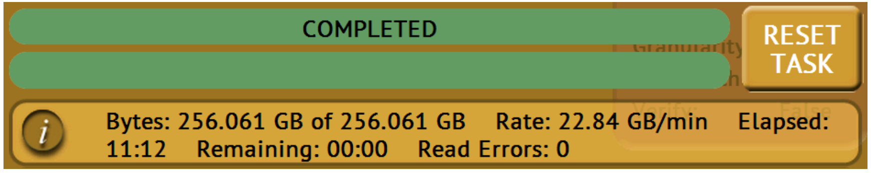
For in-depth information regarding drive encryption, please see **Chapter 8: Drive Encryption and Decryption**

6. Tap the ***Start*** icon to start the imaging task.
7. A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, and time remaining.



Bytes: 15.024 GB of 256.061 GB Rate: 22.83 GB/min Elapsed: 00:39 Remaining: 10:33 Read Errors: 0

8. When finished, the status will show "COMPLETED". At this point, it is recommended to tap ***Reset Task*** to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.



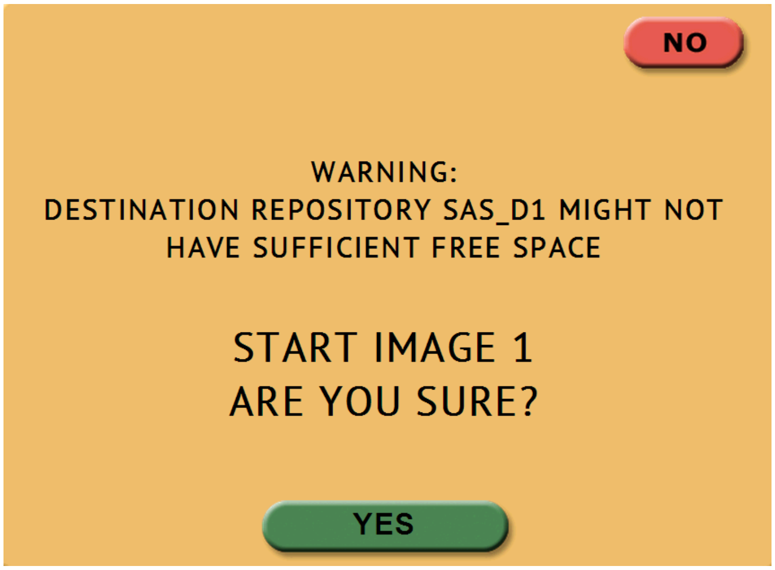
Bytes: 256.061 GB of 256.061 GB Rate: 22.84 GB/min Elapsed: 11:12 Remaining: 00:00 Read Errors: 0

The number of bytes shown on the progress bar is not the actual size of the drive. This is the actual data being processed. When 'Verify' is set to "Yes", the reported number will double in size.

For parallel imaging, prior to starting the first task, users must set all other tasks that need to be run in parallel. When all other tasks to be run in parallel are set, a confirmation screen will appear stating there are multiple tasks setup with the same Source drive.

3.1.1.1 Drive Spanning

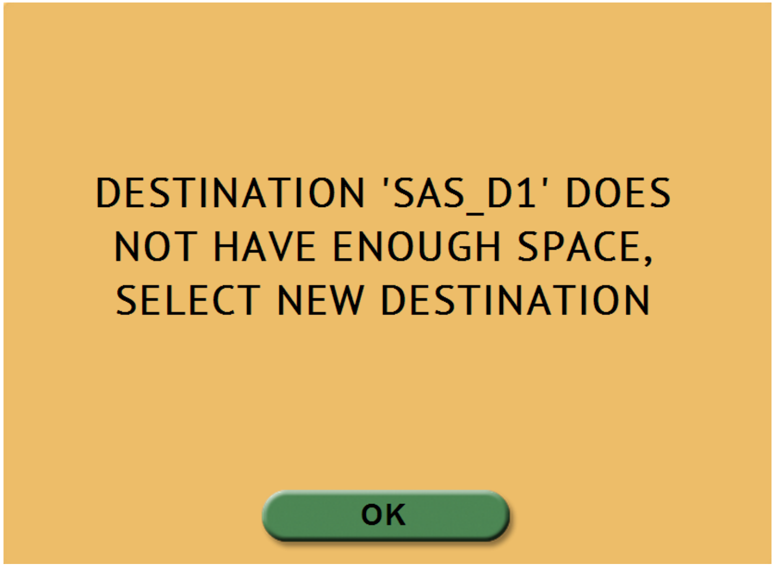
Falcon can automatically span to two (or more) Destination drives when using 'Drive to File' mode (DD, E01, EX01). When the task is started, and there may not be enough space on the Destination drive, the following prompt will appear warning that there might not be sufficient space on the Destination drive:



WARNING:
DESTINATION REPOSITORY SAS_D1 MIGHT NOT
HAVE SUFFICIENT FREE SPACE

START IMAGE 1
ARE YOU SURE?

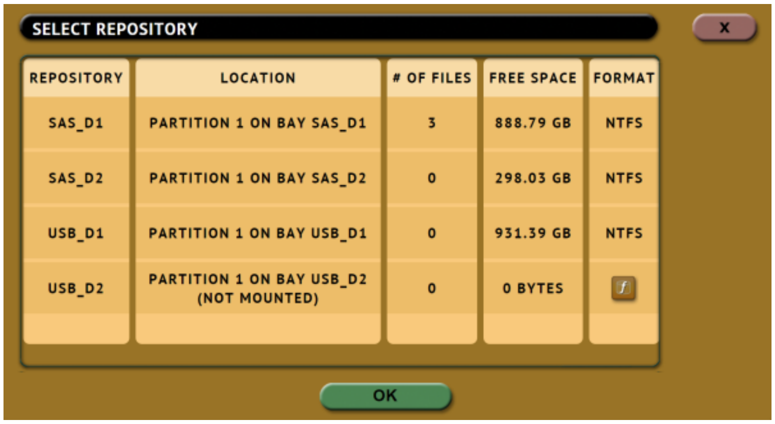
When the Destination drive is full and the remaining data to be will not fit, Falcon will prompt for another drive.



DESTINATION 'SAS_D1' DOES
NOT HAVE ENOUGH SPACE,
SELECT NEW DESTINATION

When the screen above appears, tap the ***OK*** icon and the ***Select Repository*** screen will appear. The Destination drive that is full can be disconnected, and replaced with another drive, or a different Destination drive port or repository can be selected. After selecting the next Destination/Repository to be used, tap the ***OK*** icon.

If the next Destination drive selected requires formatting, the Falcon will show the f ***(format)*** icon allowing the drive to be formatted.



SELECT REPOSITORY

REPOSITORY	LOCATION	# OF FILES	FREE SPACE	FORMAT
SAS_D1	PARTITION 1 ON BAY SAS_D1	3	888.79 GB	NTFS
SAS_D2	PARTITION 1 ON BAY SAS_D2	0	298.03 GB	NTFS
USB_D1	PARTITION 1 ON BAY USB_D1	0	931.39 GB	NTFS
USB_D2	PARTITION 1 ON BAY USB_D2 (NOT MOUNTED)	0	0 BYTES	f

When the imaging operation is finished, all subsequent Destinations/Repositories used will contain the same Case/File name and the next DD, E01, or EX01 file. For example, if the last file on the first Destination used is *.E23, the next Destination/Repository used will start with file *.E24.

3.1.2 Imaging to or from a network

A network repository or location must be set in order for the Falcon to be able to image to or from a network repository/location.

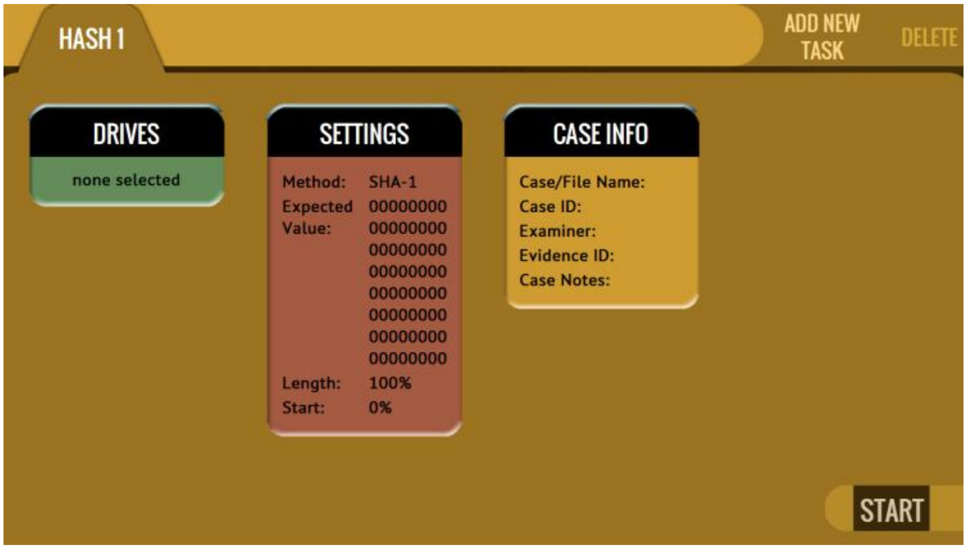
For details on how to add a network repository/location, please see **Section 6.0.10** of this manual.

3.2 Hash

A hash operation can be performed to any drive connected to the Falcon. Performing a hash task will instruct the Falcon to calculate the hash for the specified drive or validate the hash value for that drive.

Each hash task is Logical Block Address (LBA) based and will hash drives based on the number of LBAs. If multiple drives are selected to be hashed, the Falcon will hash up to the LBA value of the smallest capacity drive. If drives with different capacities need to be hashed, it is recommended to start one task per drive.

3.2.1 Step-by-step instructions – Hash



none selected

Method: SHA-1
Expected Value: 00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
Length: 100%
Start: 0%

Case/File Name:
Case ID:
Examiner:
Evidence ID:
Case Notes:

1. Select ***Hash*** from the types of operation on the left side.
2. Tap the ***Drives*** icon and select the drive(s) to be hashed then tap the ***OK*** icon.
3. Tap the ***Settings*** icon to select the hash method or algorithm. Choose from SHA-1, SHA-256 or MD5 (SHA-1 or SHA-256 are the recommended algorithms).
4. Leave the expected value at zeros to hash the drive. If the drive needs to be verified against a known/expected hash, change the expected value by tapping the ⓔ ***(edit)*** icon. Tap the ***OK*** icon to continue.
5. Change any of the optional settings (LBA settings or percentage of the drive to be hashed) if needed.
6. Optional: Tap Case Info to set the Case/File Name, Case ID, Examiner, Evidence ID, or Case Notes.

The Falcon will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

7. Tap the ***Start*** icon to start the hash task.
8. When finished, the status will show "COMPLETED". At this point, it is recommended to tap Reset Task to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.

3.3 Wipe/Format

Destination drives can be wiped and formatted using the Falcon. When a drive is wiped, there will be no file system on the Destination drive. The Destination drive must be formatted in order for it to have a valid file system so it can be used as a Destination drive when using the Drive to File or File to File modes of imaging. The following methods are available in the Wipe menu:

- ***Secure Erase*** – Sends a command to the drive instructing it to wipe the drive based on the hard drive manufacturer's specifications for the Secure Erase command.

  > If errors appear when performing Secure Erase, contact the drive manufacturer to check if the drive supports Secure Erase. For Secure Erase specifications (what happens when the drive receives the Secure Erase command), contact the drive manufacturer.

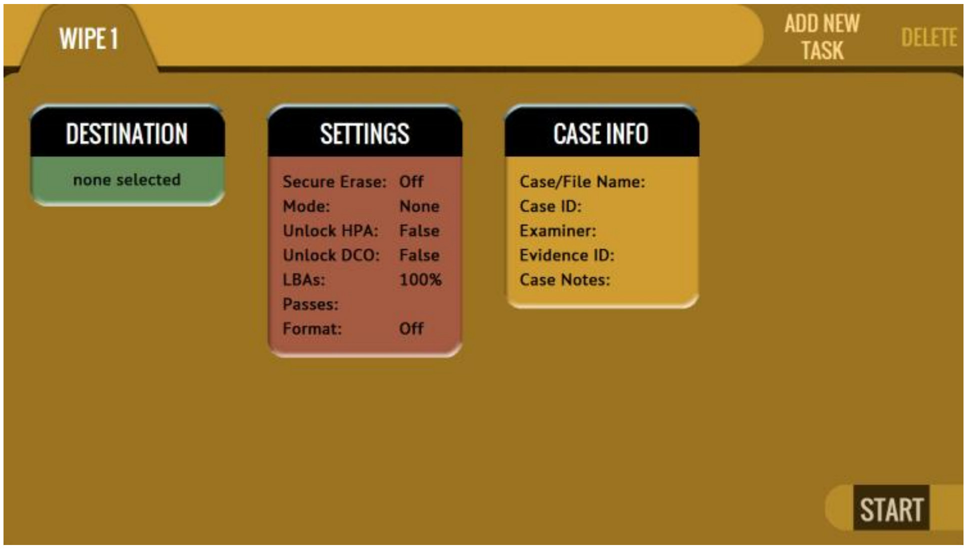
- ***Wipe Patterns*** – Allows the user to set a specific pattern to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set with pre-selected pass values.

  > It is recommended to use the same capacity drive per task. When smaller capacity drives are wiped together with larger capacity drives, the smaller drives will finish first. However, the drive bays will not be available until the entire task is finished.

- ***Format*** – Instructs the Falcon to format a drive (with or without encryption). The Falcon will format the drive using the EXT4 file system or NT file system (NTFS). To simply format a drive without wiping, set ***Secure Erase*** to ***Off*** and set the ***Wipe Patterns*** to ***None***.

  > For in-depth information regarding drive encryption, please see **Chapter 8: Drive Encryption and Decryption**. Step-by-step instructions on how to encrypt a drive can be found in **Section 8.1.1.**

3.3.1 Step-by-step instructions – Wipe/Format



none selected

Secure Erase:	Off
Mode:	None
Unlock HPA:	False
Unlock DCO:	False
LBAs:	100%
Passes:	
Format:	Off

Case/File Name:
Case ID:
Examiner:
Evidence ID:
Case Notes:

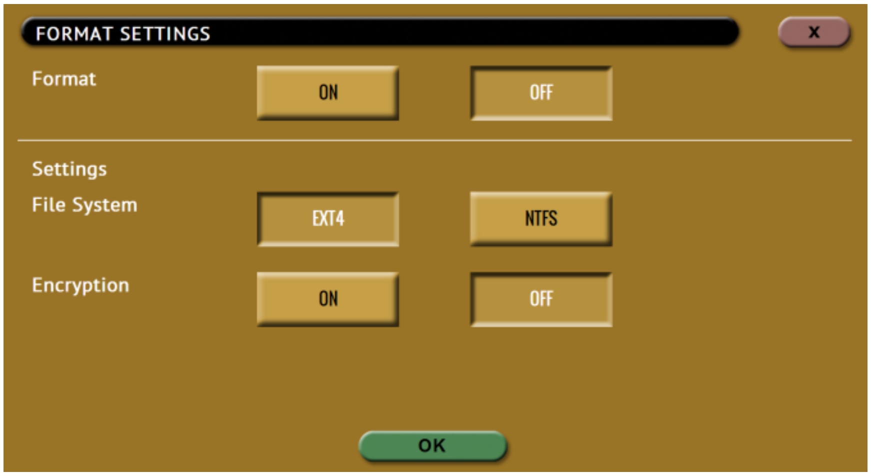
1. Select ***Wipe*** from the types of operation on the left side.
2. Tap the ***Destination*** icon and select one or more drives then tap the ***OK*** icon.

> It is recommended to use the same capacity drive per task. When smaller capacity drives are wiped together with larger capacity drives, the smaller drives will finish first. However, the drive bays will not be available until the entire task is finished.

3. Tap the ***Settings*** icon and choose the type of wipe to be performed (Secure Erase and/or Wipe Patterns). If Wipe Patterns is selected, choose the type of Wipe Pattern to perform (DoD or Custom).
4. If the drive has an HPA or DCO area that needs to be wiped, tap the ***HPA/DCO*** icon and select ***Yes*** to wipe the HPA/DCO area of the drive.
5. Tap the ***Passes*** icon to edit the number of passes and what gets written on each pass.

> If ***Custom*** was selected, at least one pass must be edited and chosen. If ***DoD*** was selected, a 7th pass value must be edited/entered.

6. If the drive needs to be formatted, tap the ***Settings*** icon to change the Format settings then tap the ***OK*** icon.



- **FORMAT –** Select ON or OFF to format the drive.
- **FILE SYSTEM –** Select whether the Falcon will format the drive with the EXT4 or NT File System (NTFS).
- **ENCRYPTION –** Select whether to encrypt the drive (ON) or not (OFF).

For more information on encrypted Destination drives, please see **Chapter 8: Drive Encryption and Decryption**.

The Falcon encrypts drives using AES 256 encryption regardless of what cipher mode is used. If TC-XTS is used, Falcon uses a TrueCrypt friendly format and does not use TrueCrypt to encrypt the drive. The encryption key is not stored on the Destination drive.

7. Optional: Tap Case Info to set the Case/File Name, Case ID, Examiner, Evidence ID, or Case Notes.

The Falcon will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

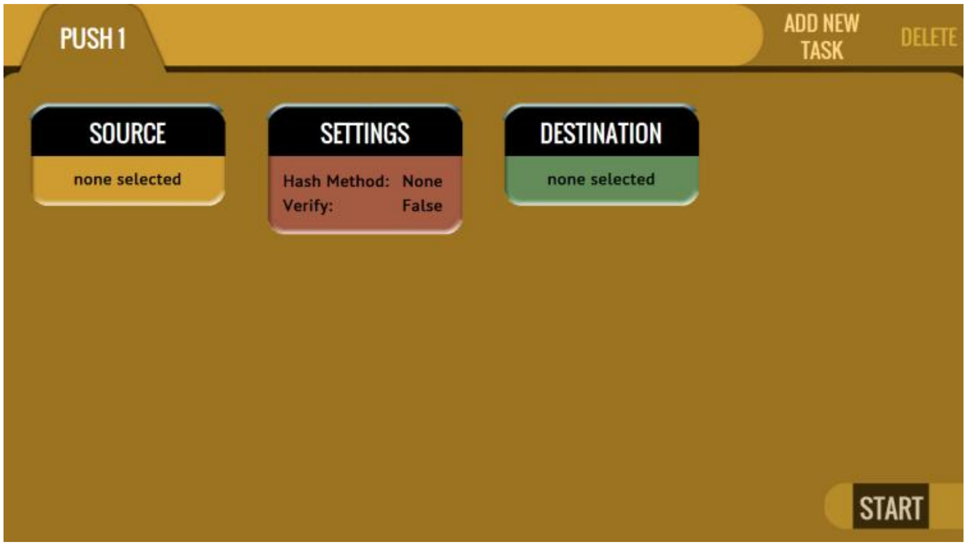
Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

8. Tap the ***Start*** icon to start the wipe task. The Falcon will perform a Secure Erase first (if selected), then a Wipe Pattern (if selected), then finally a Format (if selected).
9. When finished, the status will show "COMPLETED". At this point, it is recommended to tap Reset Task to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.

3.4 Push

The network Push operation gives users the ability to push Falcon created evidence files from destination drives connected to the Falcon or from a Falcon repository to a network location or another connected destination drive. The Push feature provides a more secure method than simply copying files through a computer by performing an SHA-1 or MD5 hash during the push process. Additionally users can select to verify the file transfer to ensure data integrity. The Falcon will generate a log file for each push process.

3.4.1 Step-by-step instructions - Push



SOURCE: none selected

SETTINGS: Hash Method: None; Verify: False

DESTINATION: none selected

To push files to a network location, a network repository must be set up. Details on how to add a repository can be found in ***Section 6.0.10.1***.

Follow these steps to set up a Push operation:

1. Select ***Push*** from the types of operation on the left side.
2. Tap the ***Source*** icon and select the drive that contains the files to be pushed then tap the ***OK*** icon.

   The Source selection will only show drives connected to the Destination ports, or locations set up as a repository.

3. A 'Select Cases' screen will appear showing each case name located on the selected source. Select one or more cases by tapping each case name. When finished, tap the ***OK*** icon.
4. Tap the ***Settings*** icon to select the hash method or algorithm. Choose from NONE, SHA-1, or MD5 and choose whether to verify the data or not (YES or NO). Tap the ***OK*** icon to continue.

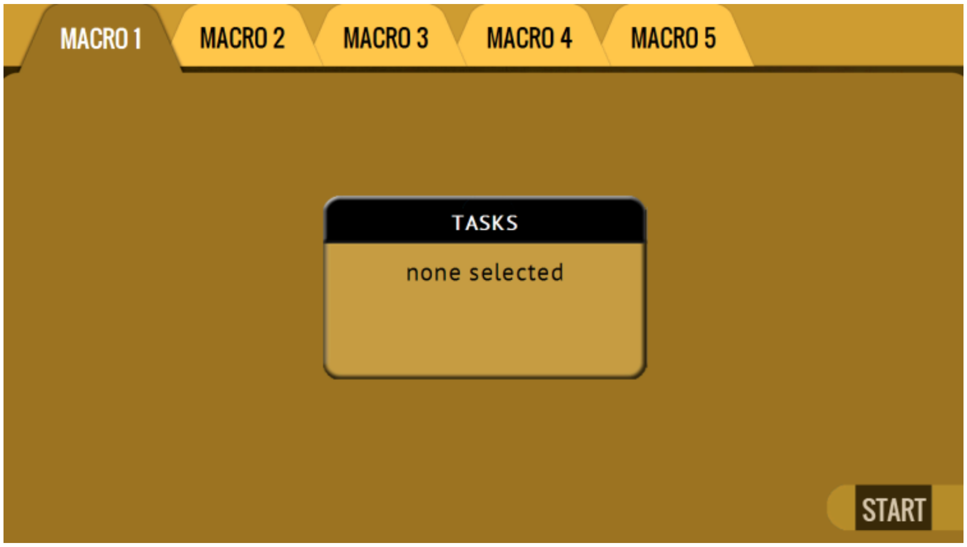
5. Optional: Tap ***Case Info*** to set the Case/File Name, Case ID, Examiner, Evidence ID, or Case Notes.
6. Verify the settings then tap the ***OK*** icon to continue.
7. Tap the ***Destination*** icon and select the destination or repository to push the images to. Tap the ***OK*** icon to continue.
8. Tap the ***Start*** icon to start the push task.
9. When finished, the status will show "COMPLETED". At this point, it is recommended to tap Reset Task to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.

Push speeds will vary depending on network conditions.

3.5 Task Macros

This operation allows up to five (5) macros that can be set. Each macro can run up to nine (9) tasks sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe, Image, and then Hash.

3.5.1 Step-by-step instructions – Task Macros



TASKS

none selected

Each task or operation must be set up before setting up the macro. For example, to set up a Task Macro that will perform a wipe, then image, users must first set up both the wipe and image tasks. Once the wipe (for example, Wipe 1) and image (for example, Image 1) has been set up, the Task Macro can be set.

1. Select ***Task Macro*** from the types of operation on the left side.
2. Select a macro (Macro 1 through Macro 5).

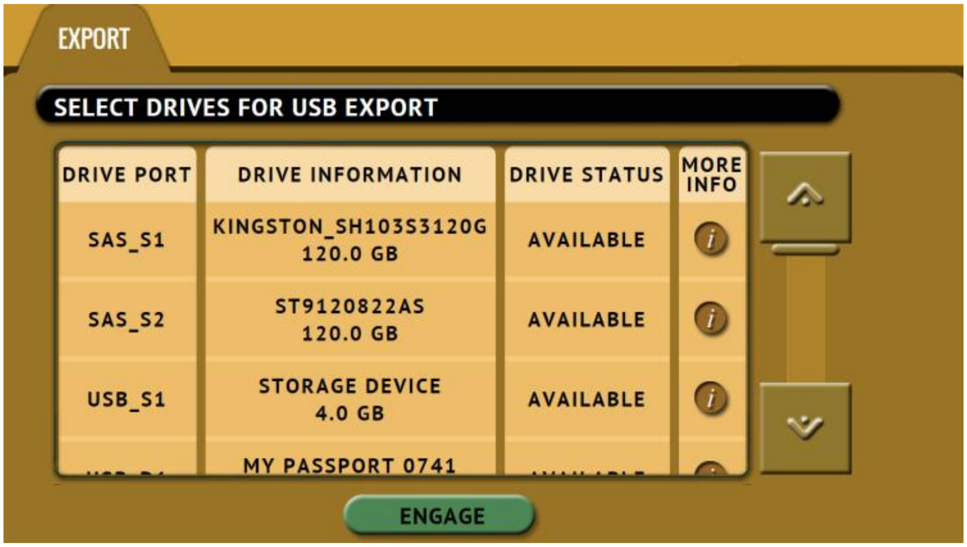
3. Tap the ***Task*** icon to select up to nine (9) operations.
4. Set up to 9 operations by tapping on each operation in order (Operation 1, Operation 2, etc.)
5. When all the operations have been set, tap the ***OK*** icon.
6. Tap the ***Start*** icon to execute the macro and perform all the operations within that macro.
7. When finished, the status will show “COMPLETED”. At this point, it is recommended to tap Reset Task to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.

3.6 USB Device (Viewing drive contents in Windows)

Connecting the Falcon to a computer via USB allows the user to view any drive connected to the Falcon. In this mode, all drives connected to the Falcon are write-protected.

Falcon formats the drives using the EXT4 file system or NT file system (NTFS). EXT4 is not natively supported by Windows. There are several utilities that allow viewing of the EXT4 file system in Windows. Logicube has tested and recommends ***Ext2Fsd*** (http://www.ext2fsd.com/) which is a utility driver that allows EXT partitions to be viewable in Windows. For detailed instructions on Ext2Fsd, please see **Chapter 7**. NTFS is natively supported by Windows.

3.6.1 Step-by-step instructions – USB Device

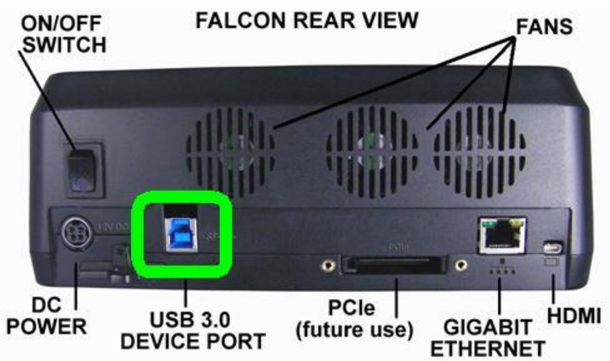


SELECT DRIVES FOR USB EXPORT

DRIVE PORT	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_S1	KINGSTON_SH103S3120G 120.0 GB	AVAILABLE	ⓘ
SAS_S2	ST9120822AS 120.0 GB	AVAILABLE	ⓘ
USB_S1	STORAGE DEVICE 4.0 GB	AVAILABLE	ⓘ
	MY PASSPORT 0741		

1. Select ***USB Device*** from the types of operation on the left side.
2. A list of drives connected to the Falcon will appear. Select a drive then tap the ***Engage*** icon.
3. Connect a USB 3.0 cable (A-to-B) between a computer and the Falcon. Connect the A connector side of the cable to an available USB port on

the computer, and connect the B connector side of the cable to the back panel of the Falcon.



4. Windows will automatically detect the drive, install the drive's drivers (if necessary), and should assign it a drive letter.
5. The new drive letter will contain the contents of the selected drive and is write-protected.
6. When finished, tap the ***Disengage*** icon on the Falcon. The USB cable can then be disconnected from the Falcon and the computer.

Windows may look like changes can be made to the drive. However, no changes are actually made. For example, if a file is written/copied to the drive, or a file is deleted from the drive, Windows may show that the file was written/copied or deleted from the drive. However, if the drive is disconnected, then reconnected, Windows will show the original files showing no changes were actually made.

3.7 File Browser

FILE BROWSER

The contents of all connected Source and Destination drives on the Falcon can be previewed using the Falcon's file browser. The Falcon will show the partitions and the contents of each partition. Note that only some files can be opened by the Falcon. Files opened by the file browser will not alter the drive in any way.

If a file cannot be previewed, the following message will appear:

File viewer cannot view file type:

3.7.1 Step-by-step instructions – File Browser

1. From the File Browser screen, select the drive to browse by tapping the corresponding tab at the top of the screen. The Falcon will show all the partitions that can be read.

2. Tap the partition to browse. The Falcon will show the contents (folders/directories and files).
3. To view a file, tap the filename. The Falcon will attempt to open the file.
    - If the Falcon can open the file, it will be displayed on the screen.
    - If the Falcon cannot open the file, a message will appear stating "File viewer cannot view file type:"

For detailed information on how to use the file browser and important notes, see *Section 6.0.7* of this manual.

3.8 Logs

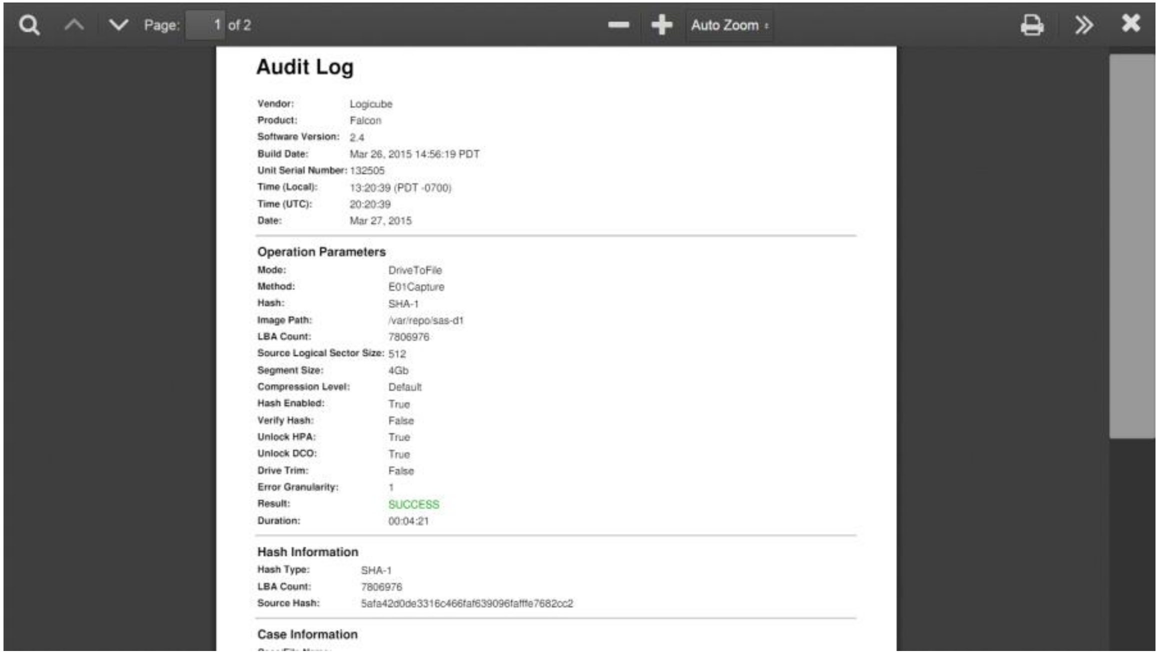
The Falcon keeps logs of all imaging, hash, wipe, format, and push operations. Logs can be viewed directly on the Falcon or from a computer's browser (if the Falcon is connected to a network). In addition to viewing, the logs can be exported to an external USB location such as a USB flash drive. Logs are exported in PDF, HTML and XML format.

When using Drive to File mode (DD, E01, or EX01), log files are also stored in the Destination drive in the same folder as the image files.

The log files in the Destination drive are available in PDF, HTML, and XML formats.

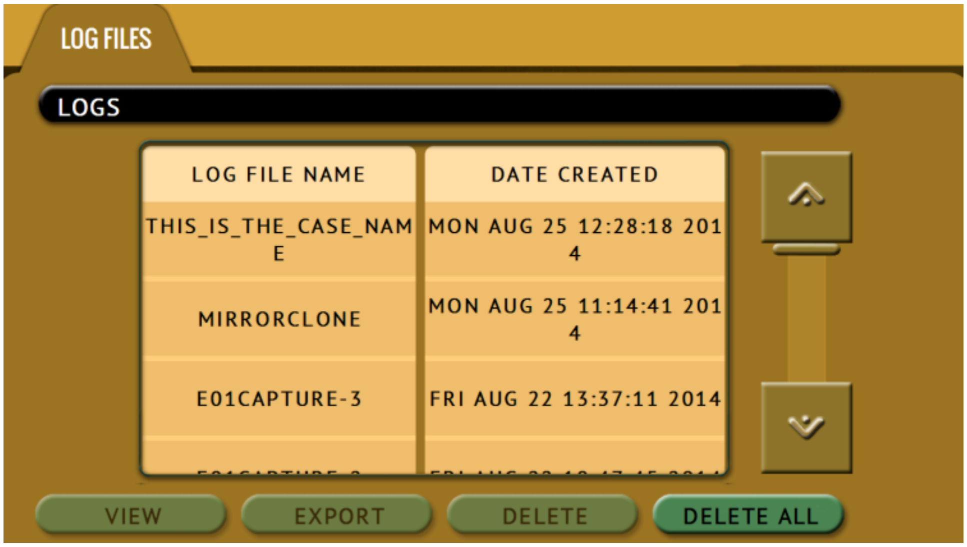
The log files may contain a "partial hash". This hash is for Falcon's internal purposes only and cannot be validated by any other means. The partial hash is a snapshot of the hash engine at the end of each segment file which the Falcon can use to catch transfer errors and re-try if needed.

Sample Log File (viewed on-screen):



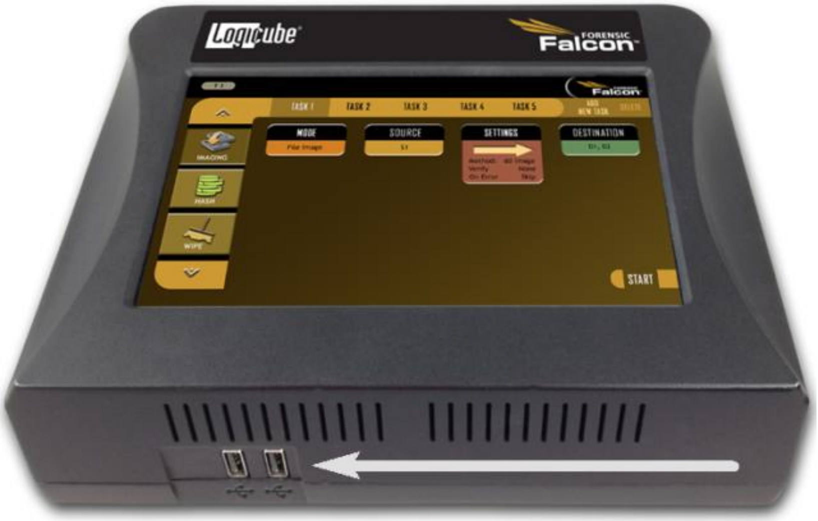
```
Audit Log

Vendor:                 Logicube
Product:                Falcon
Software Version:       2.4
Build Date:             Mar 26, 2015 14:56:19 PDT
Unit Serial Number:     132505
Time (Local):           13:20:39 (PDT -0700)
Time (UTC):             20:20:39
Date:                   Mar 27, 2015

Operation Parameters
Mode:                        DriveToFile
Method:                      E01Capture
Hash:                        SHA-1
Image Path:                  /var/repo/sas-d1
LBA Count:                   7806976
Source Logical Sector Size:  512
Segment Size:                4Gb
Compression Level:           Default
Hash Enabled:                True
Verify Hash:                 False
Unlock HPA:                  True
Unlock DCO:                  True
Drive Trim:                  False
Error Granularity:           1
Result:                      SUCCESS
Duration:                    00:04:21

Hash Information
Hash Type:          SHA-1
LBA Count:          7806976
Source Hash:        5afa42d0de3316c466faf639096tafffe7682cc2

Case Information
```

3.8.1 Step-by-step instructions – Viewing or exporting logs



LOG FILE NAME	DATE CREATED
THIS_IS_THE_CASE_NAME	MON AUG 25 12:28:18 2014
MIRRORCLONE	MON AUG 25 11:14:41 2014
E01CAPTURE-3	FRI AUG 22 13:37:11 2014

1. Select ***Logs*** from the types of operation on the left side. A list of log files will appear sorted by date (newest on top).
2. Select the log file to view by tapping the name of the log file. This will highlight the log file chosen.
3. Tap the ***View*** icon to view the log file on-screen. The log files can also be exported to a USB drive. To export the log files:
    a. Connect a USB drive (USB flash drive or USB external drive) to one of the two USB ports located on the front of the Falcon.



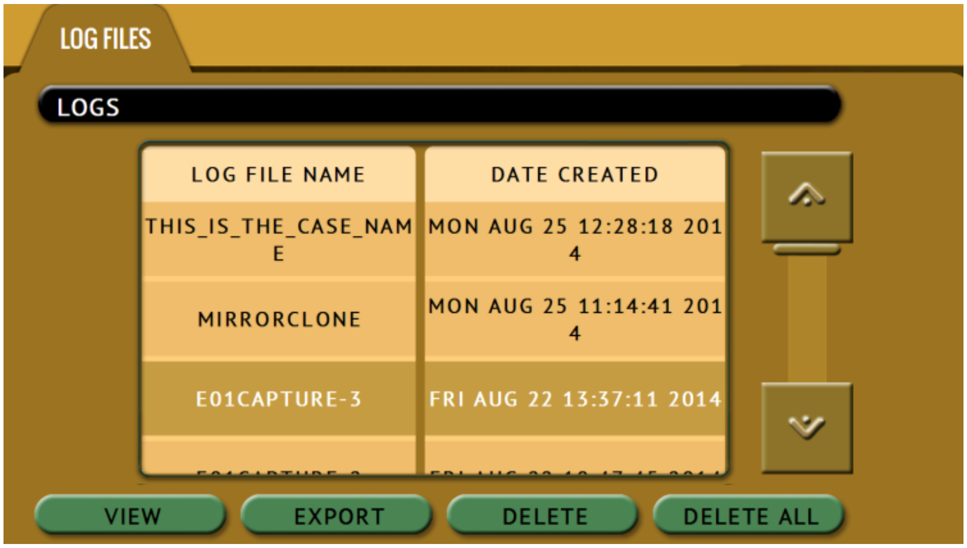
The USB drive must be formatted with the FAT, FAT32, NTFS, or EXT4 file system.

    b. Tap the ***Export*** icon to export the log file via USB. The log will be exported/copied to the attached USB drive and will be in HTML, PDF, and XML formats.

Repeat steps 2 through 4 if other log files need to be exported or viewed.

To print the log files, use the web interface as described in **Chapter 10: Remote Operation** and click the print icon on the upper-right corner of the screen. The browser's print menu will appear and the log can be printed to an available printer on configured on the computer.

3.8.2 Deleting log files



LOG FILE NAME	DATE CREATED
THIS_IS_THE_CASE_NAME	MON AUG 25 12:28:18 2014
MIRRORCLONE	MON AUG 25 11:14:41 2014
E01CAPTURE-3	FRI AUG 22 13:37:11 2014
E01CAPTURE-2	FRI AUG 22 10:47:15 2014

Log files can be deleted one at a time or all at once.

- To delete a single log file, tap the log file to highlight the log file to be deleted. Tap the ***Delete*** icon to delete the selected log file.
- To delete all the log files, tap the ***Delete All*** icon.

A log file deletion password can be set to add a layer of security when deleting log files. If a password was set, log files cannot be deleted without entering the correct password.

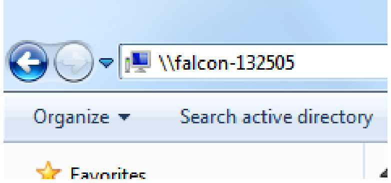
- If a log file deletion password was not created, a confirmation screen will appear confirming to delete the single log file or all log files.
- If a log file deletion password was created, a screen will appear prompting to enter the log file deletion password. Enter the log file deletion password. Tap the ***OK*** icon to delete the single log file or all the log files (depending on which was selected).

The password can be set in the ***Systems Settings***. More information about the log file deletion password can be found in ***Section 6.0.11.2***.

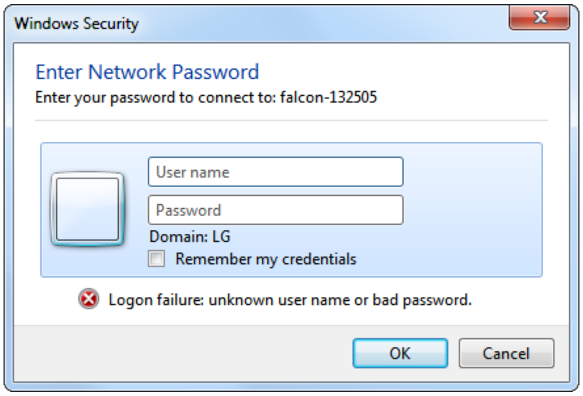
3.8.3 Accessing the logs over a network

The log files can also be accessed through a network on a computer if the Falcon is connected on the same network.

1. Open Windows Explorer or a similar window and browse to the hostname or the IP address found in the Statistics screen. See ***Section 6.0.9*** for more information on the Statistics screen.



2. A Windows security screen will appear prompting to enter a User name and Password to connect to the Falcon. Login with the following credentials:
   - User name: ***it***
   - Password ***it***



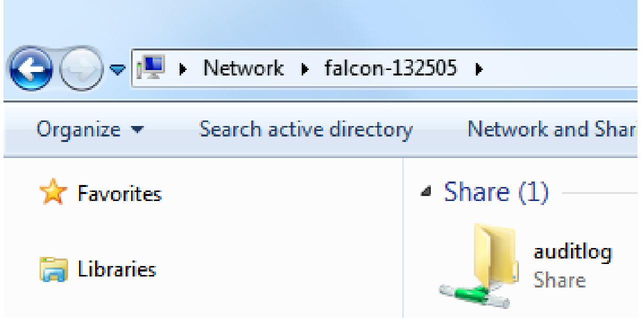
Enter Network Password

Enter your password to connect to: falcon-132505

Domain: LG

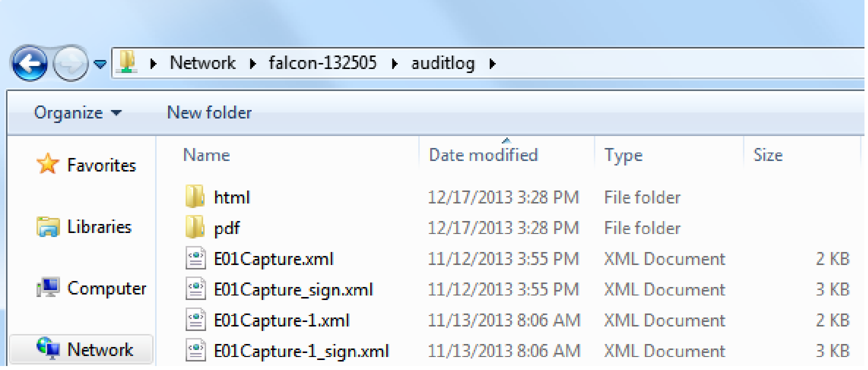
Logon failure: unknown user name or bad password.

3. Once connected, an ***auditlog*** folder will appear. Open the ***auditlog*** folder.



4. The auditlog folder contains the HTML, PDF, and XML files for each of the log files. There will be two folders (html and pdf) that contain either the HTML or PDF versions of the log files. The XML files can be used with

any XML viewer which allows for some customization on how the information can be viewed.



Name	Date modified	Type	Size
html	12/17/2013 3:28 PM	File folder	
pdf	12/17/2013 3:28 PM	File folder	
E01Capture.xml	11/12/2013 3:55 PM	XML Document	2 KB
E01Capture_sign.xml	11/12/2013 3:55 PM	XML Document	3 KB
E01Capture-1.xml	11/13/2013 8:06 AM	XML Document	2 KB
E01Capture-1_sign.xml	11/13/2013 8:06 AM	XML Document	3 KB

3.9 Statistics (Falcon and drive statistics)

FORENSIC Falcon STATISTICS

This will display two tabs: ***About*** and ***Adv. Drive Statistics***.

The ***About*** screen will show information about the Forensic Falcon including the current software installed.

The ***Adv. Drive Statistics*** tab displays S.M.A.R.T. information taken directly from what the drive is reporting.

For more information on the Statistics screen, see **Section 6.0.9** of this manual.

3.10 Manage Repositories

MANAGE REPOSITORIES

Repositories can be added to the Falcon in this operation. When ***Manage Repositories*** is selected, a list of repositories will be shown. The user has the option of adding or deleting a repository.

For more information on how to manage repositories, see **Section 6.0.10** of this manual.

3.11 System Settings

SYSTEM SETTINGS

The ***System Settings*** screen allows users to configure five different settings for the Falcon:

- User Profiles/Configurations

- Passwords
- Encryption Settings
- Language/Time Zone
- Display

For more information on Falcon’s system settings, see **Section 6.0.11** of this manual.

3.12 Network Settings

http:// NETWORK SETTINGS

There are two tabs in the Network settings screen:

- Services – The network settings screen allows certain network services to be enabled or disabled.
- HTTP Proxy – In order for the Falcon to be able to update software from a network (over the internet), a proxy settings may need to be set. Networks that have a proxy server for internet access will require proxy settings for devices like the Falcon to connect to the Internet. This typically includes a server (or IP address), a host port, a username and password.

For detailed information on the Network Settings screen, see **Section 6.0.12** of this manual.

3.13 Software Updates

SOFTWARE UPDATES

New and improved software will be released from time to time. There are two ways to update the software on the Falcon: From the web via a network connection or from a USB drive.

For more information on see **Chapter 9: Updating the Falcon Software**.

3.14 Power Off

POWER OFF

There are two tabs in the Power Off screen:

POWER OFF – The Falcon can be remotely turned off by going to this tab.

DRIVE POWER – Inactive drives connected to the Falcon can be set to go to standby mode in this tab. The default is set to 0 minutes (OFF).

For more detailed screen shots, see **Section 6.0.14** of this manual.

4: Previewing Drives

4.0 Previewing Drives

Drives connected to both Source and Destination ports can be previewed. There are 5 different methods available to preview drive contents with the Falcon:

- Falcon's native File Browser
- A computer + Falcon's File Browser
- USB connection to a computer
- SMB protocol (Using a file explorer)
- iSCSI protocol – Source drives only (Using a file explorer)

Drives connected to the Source ports (SAS_S1, SAS_S2, USB_S1, and FW_S1) – Drives connected to the Source ports are always write-protected. Previewing the contents of these drives will not alter the drive or its contents in any way.

	Physical Access to the Drive	Logical Access to the Drive	Access to Source Drives	Access to Destination Drives	Concurrent Multi-User Connection	Concurrent Multi-Drive Access	Use of Third Party Analysis Tools or Software
File Browser		✓	✓	✓			
Computer + File Browser		✓	✓	✓	✓	✓	Very Limited[1]
USB	✓	✓	✓	✓			✓
SMB		✓	✓	✓	✓	✓	✓
iSCSI	✓	✓	✓		✓	✓	✓

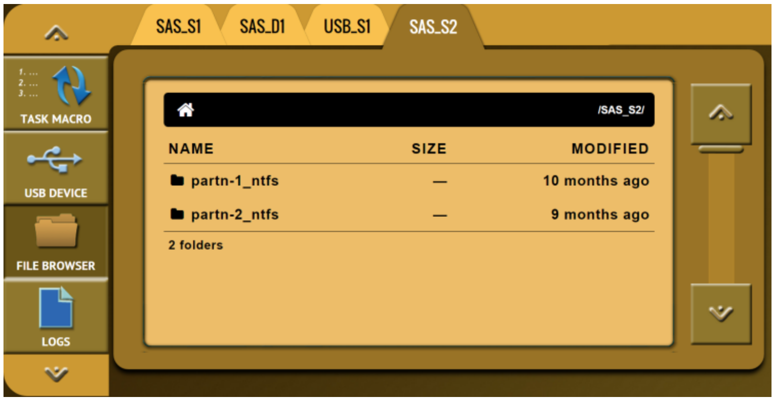
[1] One file at a time must be downloaded to the computer before it can be analyzed.

	Viewable File Types	Additional Comments
File Browser	Text, PDF, HTML, and some image files only	Drives can only be accessed on the Falcon unit itself.
Computer + File Browser	All files supported by the OS or installed software	Drives can be accessed from multiple computers if connected to a network. More powerful viewing capabilities through the computer's Operating System compared to using the File Browser alone.
USB	All files supported by the OS or installed software	Drives can only be accessed by the computer the Falcon is connected to. Drives will appear in Disk Management and can be accessed on the physical level. Partitions are searchable using the Operating System's search functions. Third party analysis tools and software can be used easily since partitions are mounted.
SMB	All files supported by the OS or installed software	Logical access to partitions viewable by the computer's Operating System. Partitions are searchable using the Operating System's search functions. Third party analysis tools and software can be used easily since partitions are mounted.
iSCSI	All files supported by the OS or installed software	Requires an iSCSI Target. Drives will appear in Disk Management and can be accessed on the physical level. Partitions are searchable using the Operating System's search functions. Third party analysis tools and software can be used easily since partitions are mounted.

4.1 File Browser

The Falcon has a built-in file browser. The built-in browser allows the user to view each of the drive's partitions and its contents. The file browser can also open several types of image files including .jpg, .png, .gif, .txt, .html, and .pdf. This method can be very useful when the Falcon is out on the field and there are no computers to analyze or triage the contents of drives. Using the Falcon's 7" touch screen, one drive at a time can be viewed.

See Section 6.0.7 for details on how to use the File Browser.



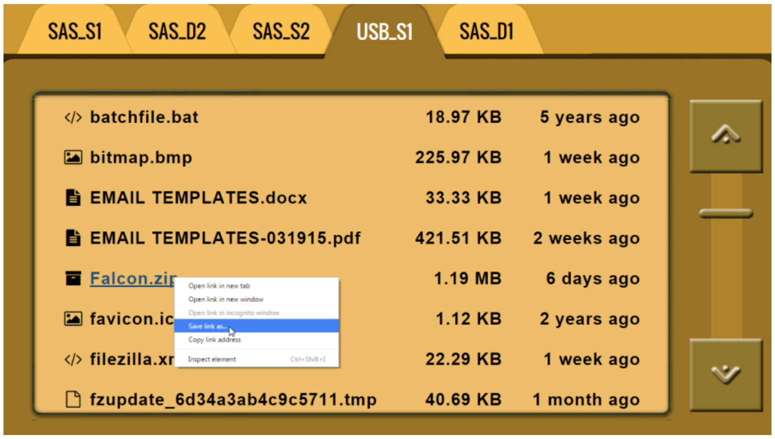
NAME	SIZE	MODIFIED
partn-1_ntfs	—	10 months ago
partn-2_ntfs	—	9 months ago

2 folders

4.2 Computer + File Browser

The Falcon can be accessed from a computer (through a direct network cable connection or through a network). Using a computer with the Falcon's file browser allows more files to be previewed by using the computer's Operating System and installed software. This can be useful when the Falcon is out on the field and there is an available laptop. Connecting the two devices directly together with a network cable, and using the Falcon's web interface (See ***Section 10.1*** for more information on the web interface) allows the user to be able to open files that the Falcon cannot open using the file browser alone.

See Section 6.0.7.1 for details on how to use the File Browser using the web interface.

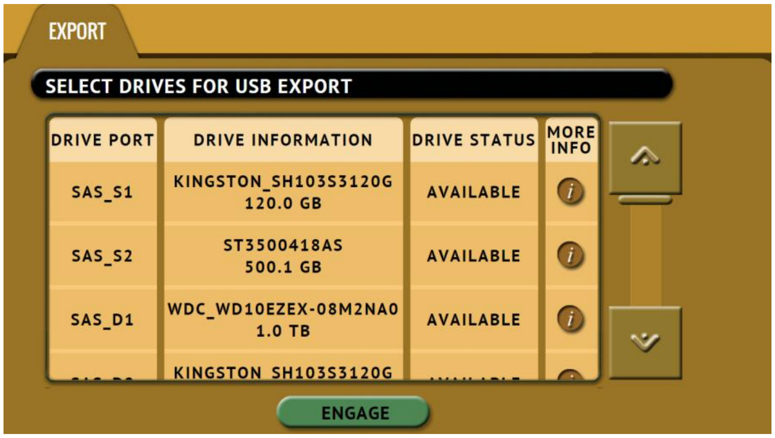


batchfile.bat	18.97 KB	5 years ago
bitmap.bmp	225.97 KB	1 week ago
EMAIL TEMPLATES.docx	33.33 KB	1 week ago
EMAIL TEMPLATES-031915.pdf	421.51 KB	2 weeks ago
Falcon.zip	1.19 MB	6 days ago
favicon.ic	1.12 KB	2 years ago
filezilla.xr	22.29 KB	1 week ago
fzupdate_6d34a3ab4c9c5711.tmp	40.69 KB	1 month ago

4.3 USB

The Falcon can also be connected to a computer through USB (the USB 3.0 port is located in the back of the Falcon). To use this method, a drive must be engaged from the Falcon using the ***USB Device*** mode of operation. The entire drive will be available to be previewed from the computer. Partitions will be viewable (For example, in Windows Explorer) and the drive will also appear in Disk Management. Using a USB connection may be useful for times when the Falcon cannot be connected over a network connection.

See Section 3.6 and 6.0.6 for details on how to use the USB Device feature.



DRIVE PORT	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_S1	KINGSTON_SH103S3120G 120.0 GB	AVAILABLE	i
SAS_S2	ST3500418AS 500.1 GB	AVAILABLE	i
SAS_D1	WDC_WD10EZEX-08M2NA0 1.0 TB	AVAILABLE	i
	KINGSTON_SH103S3120G		

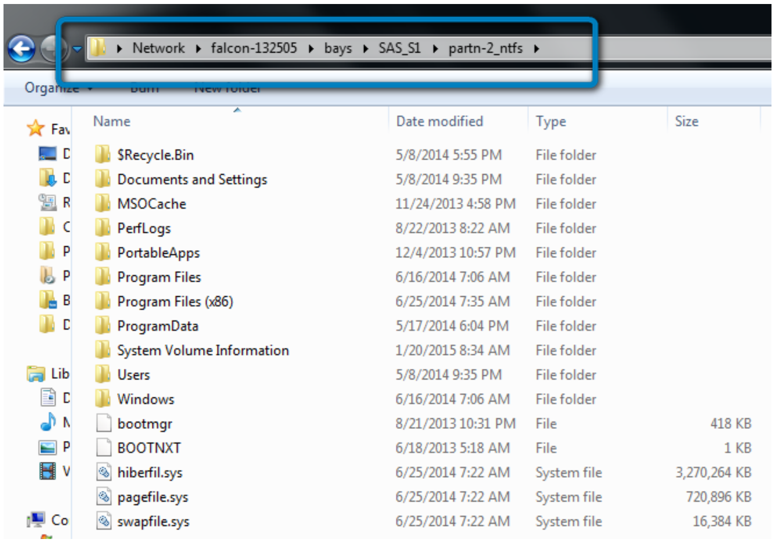
4.4 SMB

The Falcon can be accessed from a computer (through a direct network cable connection or through a network). One of the ways to access Source or Destination drives over the network is to use the SMB protocol. When using this method, all viewable/compatible partitions will be viewable on the computer. This method will give a logical access to the contents of the drive.

See Section 11.1 for details on how to view Source or Destination drives over the network using SMB.

Some advantages of using this method are:

- The contents of the drive are searchable using the Operating System's search functions.
- Third party analysis tools and software can be used with the logical partition.



Name	Date modified	Type	Size
$Recycle.Bin	5/8/2014 5:55 PM	File folder	
Documents and Settings	5/8/2014 9:35 PM	File folder	
MSOCache	11/24/2013 4:58 PM	File folder	
PerfLogs	8/22/2013 8:22 AM	File folder	
PortableApps	12/4/2013 10:57 PM	File folder	
Program Files	6/16/2014 7:06 AM	File folder	
Program Files (x86)	6/25/2014 7:35 AM	File folder	
ProgramData	5/17/2014 6:04 PM	File folder	
System Volume Information	1/20/2015 8:34 AM	File folder	
Users	5/8/2014 9:35 PM	File folder	
Windows	6/16/2014 7:06 AM	File folder	
bootmgr	8/21/2013 10:31 PM	File	418 KB
BOOTNXT	6/18/2013 5:18 AM	File	1 KB
hiberfil.sys	6/25/2014 7:22 AM	System file	3,270,264 KB
pagefile.sys	6/25/2014 7:22 AM	System file	720,896 KB
swapfile.sys	6/25/2014 7:22 AM	System file	16,384 KB

4.5 iSCSI

Another way to access Source drives from a computer (through a direct network cable connection or through a network) is through the iSCSI protocol. This method allows both physical and logical access to the drives, but may require additional software installed and configured on the computer. To use the iSCSI protocol, an iSCSI initiator must be installed and configured to view the contents of drives connected to the Falcon over a network.

Like using SMB, some advantages of using this method are:

- The contents of the drive are searchable using the Operating System's search functions.
- Third party analysis tools and software can be used with the logical partition.

See Section 11.2 for details on how to view Source drives over the network using iSCSI.

5: IMAGING

5.0 Imaging

IMAGING

This type of operation allows the imaging of a Source drive to a Destination. There are three different imaging modes and several settings to choose from. These selections should be performed in order from left to right.

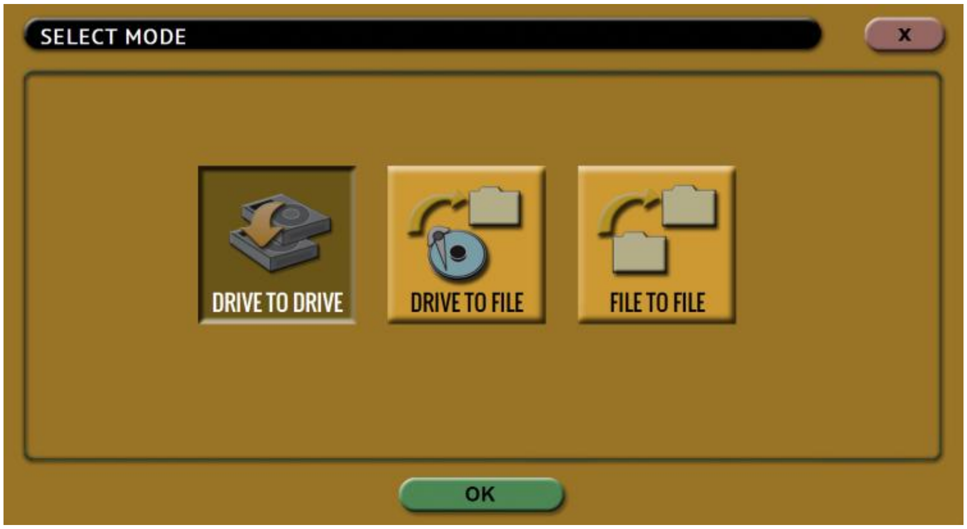
There are four selections when performing an image:

- Mode
- Source
- Settings
- Destination

5.0.1 Mode

MODE

Tap this icon to choose between the following three imaging modes:



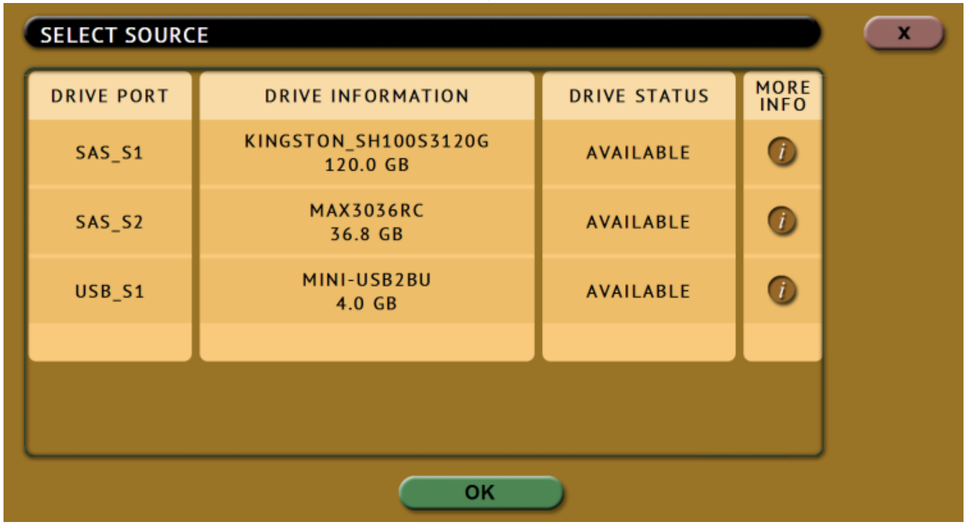
- **Drive to Drive –** Performs a bit-for-bit copy of the Source producing an exact duplicate of the Source drive.

- **Drive to File –** Images the Source to any of the following image output file formats: ***DD***, ***E01***, or ***EX01***. Compression is available for E01 and EX01 modes.
- **File to File –** Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source. If a hash method is selected, each file will be hashed.

5.0.2 Source

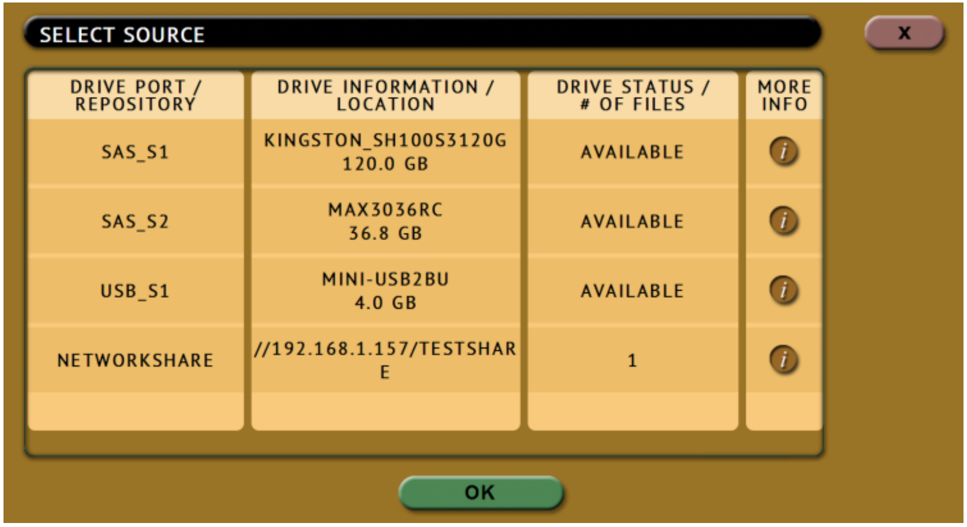
SOURCE Tap this icon to select the Source drive to be imaged. Falcon will list all the drives connected to the Source position(s).

When ***Drive to Drive*** or ***Drive to File*** mode is selected, the Source window will show all drives connected to the Source positions.



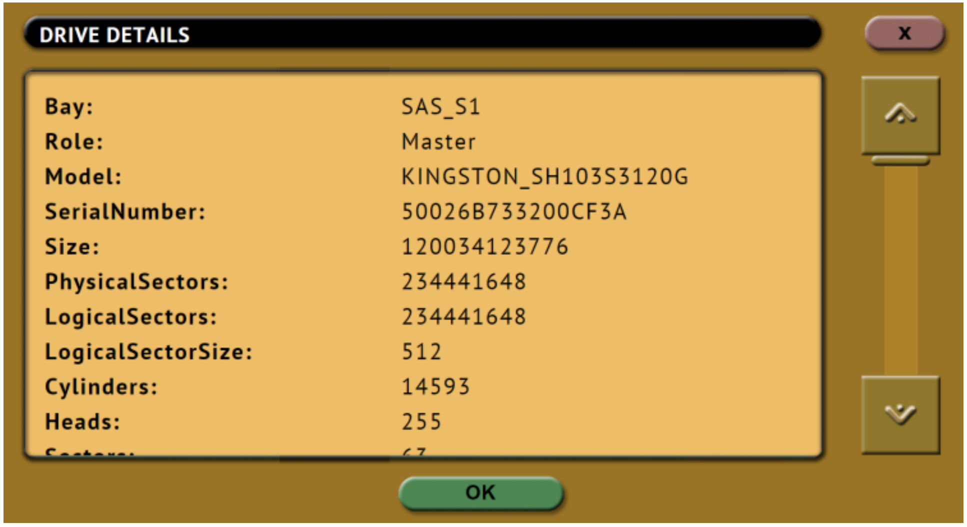
DRIVE PORT	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_S1	KINGSTON_SH100S3120G 120.0 GB	AVAILABLE	i
SAS_S2	MAX3036RC 36.8 GB	AVAILABLE	i
USB_S1	MINI-USB2BU 4.0 GB	AVAILABLE	i

When ***File to File*** mode is selected, the Source window will show all drives connected to the Source positions and any repository added with the Source role (Source or Both Source and Destination).



DRIVE PORT / REPOSITORY	DRIVE INFORMATION / LOCATION	DRIVE STATUS / # OF FILES	MORE INFO
SAS_S1	KINGSTON_SH100S3120G 120.0 GB	AVAILABLE	i
SAS_S2	MAX3036RC 36.8 GB	AVAILABLE	i
USB_S1	MINI-USB2BU 4.0 GB	AVAILABLE	i
NETWORKSHARE	//192.168.1.157/TESTSHARE	1	i

The ⓘ ***(More Info)*** icon displays more information on the drive. The drive details window will appear showing information about the drive.



Bay:	SAS_S1
Role:	Master
Model:	KINGSTON_SH103S3120G
SerialNumber:	50026B733200CF3A
Size:	120034123776
PhysicalSectors:	234441648
LogicalSectors:	234441648
LogicalSectorSize:	512
Cylinders:	14593
Heads:	255
Sectors:	63

5.0.3 Settings

SETTINGS

Tap the ***Settings*** icon to change the image settings. Depending on what Mode was selected (Drive to Drive, Drive to File, or File to File), different screens will appear.

COMMON SETTINGS – The following settings are found on all three modes:

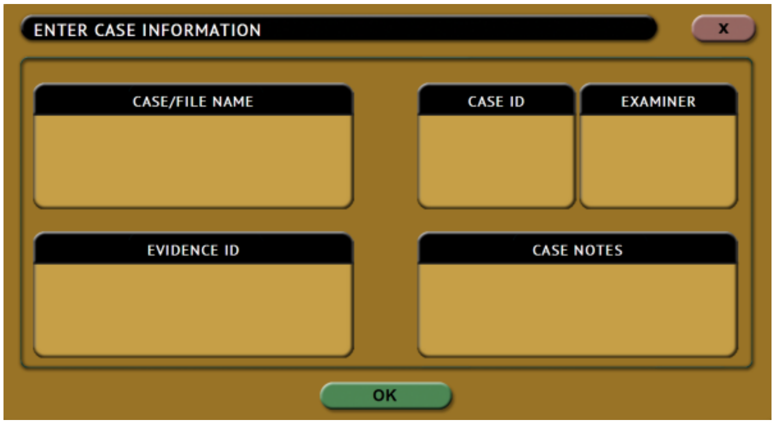
- Case Info
- HPA/DCO
- Error Handling / Error Granularity
- Hash/Verification Method

SHA-256 verification is only available when using ***Drive to Drive*** mode.

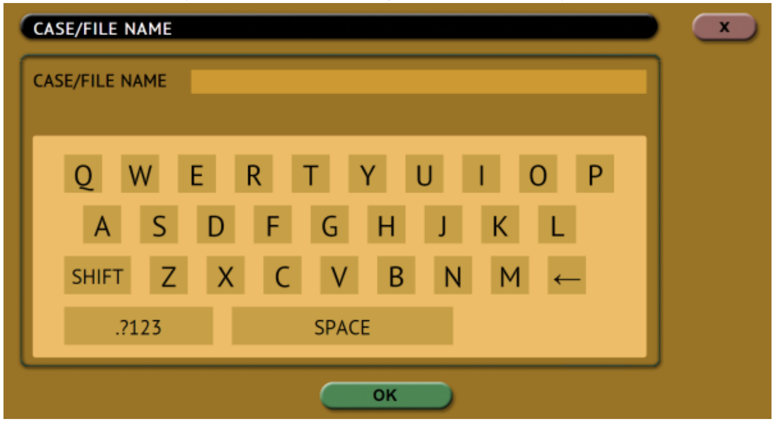
5.0.3.1 Case Info (Common Setting)

Case Info allows users to enter information about the case. This is optional and is not required to start an imaging operation.

Information entered here will appear in the logs. In addition, some forensic analysis software can import the information when the image files are opened.



Tap any of the boxes and an on-screen keyboard will appear allowing information to be entered. After entering the information, tap the ***OK*** icon to go back to the previous screen.



Log names and file names can be customized by entering a ***Case/File Name***. For example, if a DD or E01 image is performed, and the Case/File Name is set to ***TestCase***, the log name and file name will be called ***TestCase***. Subsequent Case/File Names that are the same will be identified with a dash, then the next image number, for example, TestCase-1, TestCase-2, etc.

The Falcon will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

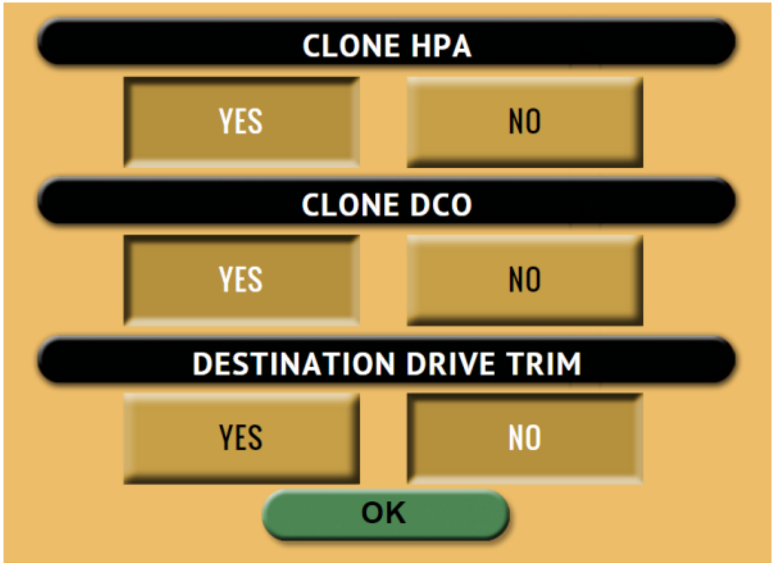
Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

5.0.3.2 HPA, DCO (Common Setting) and Drive Trim

Some computer manufacturers will use a utility that creates an HPA or DCO configuration on a hard drive. These configurations are designed to change drive characteristics such as drive capacity, speed and other settings as they are reported to the computer's BIOS.

The HPA/DCO setting allows the user to set whether a drive's HPA or DCO is to be unlocked and imaged.

Select ***YES*** to unlock and image a Host Protected Area (HPA) or Device Configuration Overlay (DCO).



CLONE HPA
YES NO
CLONE DCO
YES NO
DESTINATION DRIVE TRIM
YES NO
OK

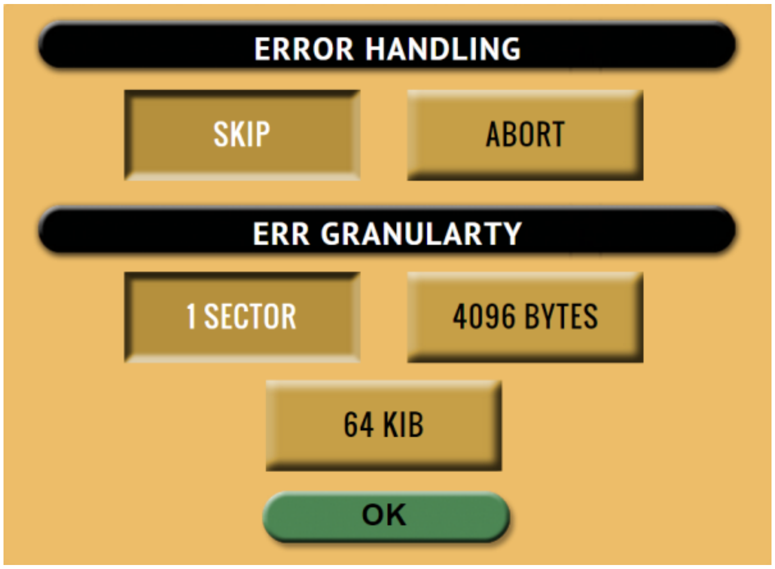
HPA – Host Protected Area can limit the size of a hard drive, but it can also change many other settings such as speed and S.M.A.R.T. status.

DCO – Device Configuration Overlay limits the size of a drive only. For example, a 160GB drive can be made to look like a 100GB drive to a computer.

Drive Trim is a special setting when the mode is set to Drive to Drive. For more information on Drive Trim, please see ***section 6.0.3.5.1 Special Settings for Drive to Drive***.

5.0.3.3 Error Handling (Common Setting)

When bad sectors are encountered on the Source drive, Falcon can either skip the bad sectors or abort the imaging operation. This allows flexibility on what to do when bad sectors are found on the Source drive.



When bad sectors are encountered, and error handling is set to ***Skip***, Falcon will write a zero on the corresponding sector or position in the Destination drive or file.

Falcon also has a setting for error granularity. There are 3 options:

- 1 sector (512 Bytes)
- 4096 Bytes (8 sectors)
- 64 KIB (128 sectors)

When a bad sector on the source drive is found, by default, it will skip that sector. Changing the granularity allows more sectors to be skipped.

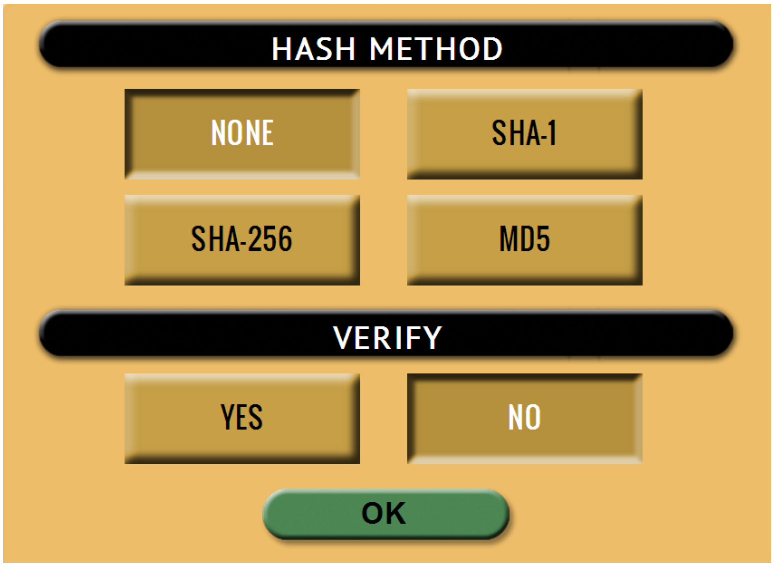
A cluster size represents the smallest amount of disk space that can be used to hold a file. The most common cluster size for an NTFS volume, for example, is 4KB (4096 Bytes). This means that the smallest amount of space that will be used for a file is 4096 Bytes.

As an example, if 4096 Bytes is chosen, and one of the 8 sectors in that cluster size contains a bad sector, the Falcon will skip the entire cluster (or 4096 bytes or 8 sectors).

5.0.3.4 Hash/Verification Method (Common Setting)

This setting allows the user to set a hash and/or a verification method.

Hash – Will hash the Source drive with the selected method. There are two, three, or four hash algorithm options available, depending on which Imaging mode or File Image Method is selected:



- **None –** No hash of the Source will be performed.
- **SHA-1 –** Uses the SHA-1 algorithm to hash the Source.
- **SHA-256 –** Uses the SHA-256 algorithm to hash the Source. This is only available when using the Drive to Drive Imaging mode.
- **MD5 –** Uses the MD5 algorithm to hash the Source.

Verification Method – Select ***YES*** to hash the Destination and verify that hash with the selected Source hash.

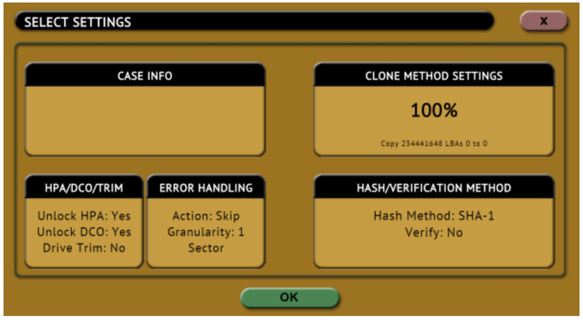
5.0.3.5 Special Settings

The Settings screen changes depending on which of the three ***Modes*** (Drive to Drive, Drive to File, or File to File) is selected. Each of the three modes has their own different ***Settings*** screen.

5.0.3.5.1 Special Settings for Drive to Drive

When ***Drive to Drive*** mode is selected, ***Mirror Settings*** will appear on the top-right of the

Settings screen:



100%

Copy 234441648 LBAs 0 to 0

Unlock HPA: Yes
Unlock DCO: Yes
Drive Trim: No

Action: Skip
Granularity: 1 Sector

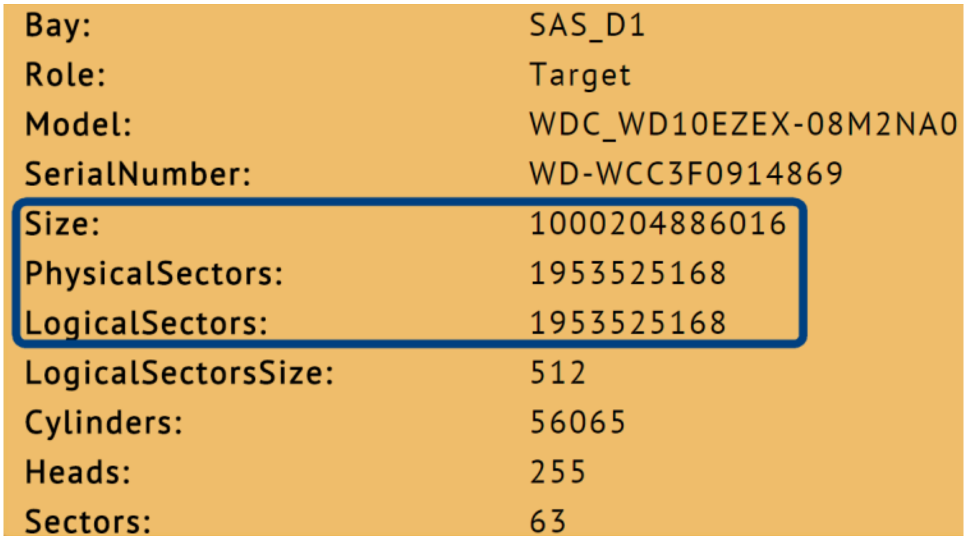
Hash Method: SHA-1
Verify: No

DRIVE TRIM – Software 2.3 and above include a feature called Drive Trim (Destination Drive Trim). This user selectable function allows the Falcon to manipulate the Device Configuration Overlay (DCO) and Host Protected Area (HPA) of the destination drive using the *Device Configuration Set* command for DCO and *Set Max Address* command for HPA so that the Destination drive's total native capacity matches the Source drive. For example, if the Source drive is a 120GB drive and the Destination drive is a 500GB drive, the Falcon will limit the Destination drive's capacity to 120GB to match the Source drive exactly.

SAMPLE SOURCE DRIVE:

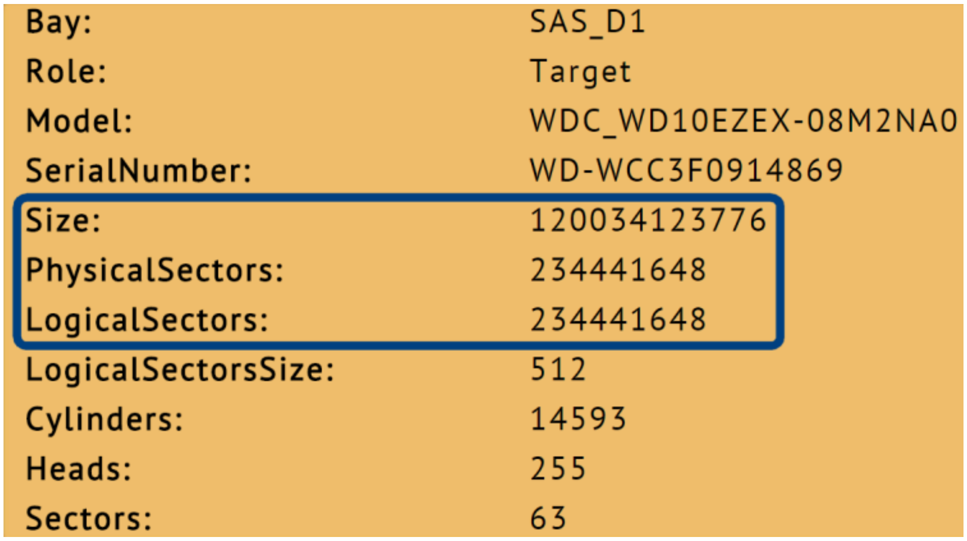
Bay:	SAS_S1
Role:	Master
Model:	KINGSTON_SH103S3120G
SerialNumber:	50026B733200CA0C
Size:	120034123776
PhysicalSectors:	234441648
LogicalSectors:	234441648
LogicalSectorsSize:	512
Cylinders:	14593
Heads:	255
Sectors:	63

SAMPLE DESTINATION DRIVE PRIOR TO DRIVE TRIM:



```
Bay:                     SAS_D1
Role:                    Target
Model:                   WDC_WD10EZEX-08M2NA0
SerialNumber:            WD-WCC3F0914869
Size:                    1000204886016
PhysicalSectors:         1953525168
LogicalSectors:          1953525168
LogicalSectorsSize:      512
Cylinders:               56065
Heads:                   255
Sectors:                 63
```

SAMPLE DESTINATION DRIVE AFTER DRIVE TRIM:



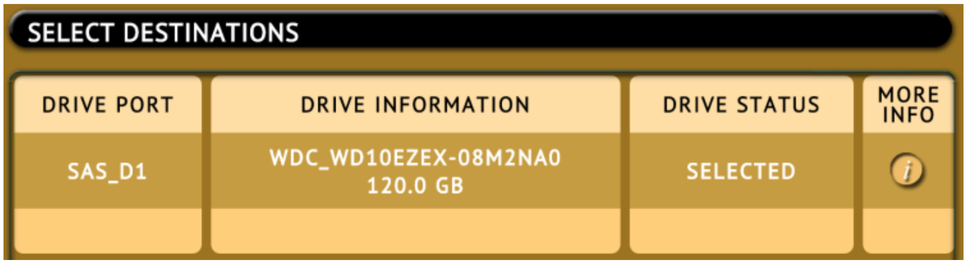
```
Bay:                     SAS_D1
Role:                    Target
Model:                   WDC_WD10EZEX-08M2NA0
SerialNumber:            WD-WCC3F0914869
Size:                    120034123776
PhysicalSectors:         234441648
LogicalSectors:          234441648
LogicalSectorsSize:      512
Cylinders:               14593
Heads:                   255
Sectors:                 63
```

Drive Trim is only available in ***Drive to Drive*** mode and by default is set to ***NO***.

Drive Trim only works with ATA drives and will not work with USB external drives (or drives connected via USB), SAS or SCSI drives.

Restoring a trimmed drive – To restore a trimmed drive to its original capacity, perform a custom wipe (single pass) and set the WIPE DCO and WIPE HPA settings to YES.

RESTORING A TRIMMED DRIVE: Select the drive to restore

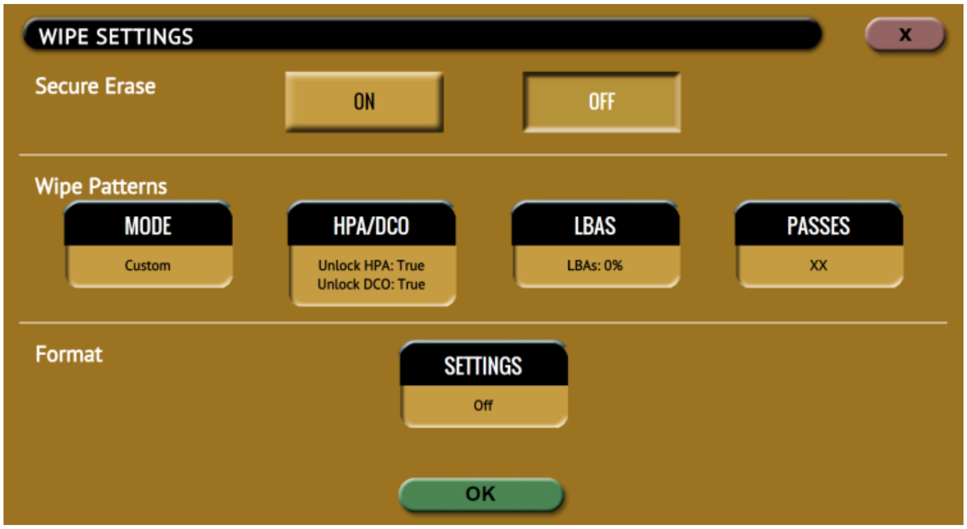


SELECT DESTINATIONS

DRIVE PORT	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_D1	WDC_WD10EZEX-08M2NA0 120.0 GB	SELECTED	i

IN THE WIPE SETTINGS:

- Set Secure Erase to OFF
- Set Wipe Patterns to:
  - Mode: Custom
  - HPA/DCO: YES (TRUE)
  - LBAS: Edit to 1 LBA
  - PASSES: Edit the number of passes to any value for 1 pass



WIPE SETTINGS

Secure Erase: ON / OFF

Wipe Patterns

MODE: Custom

HPA/DCO: Unlock HPA: True, Unlock DCO: True

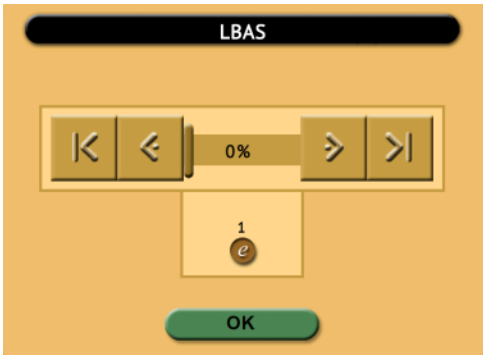
LBAS: LBAs: 0%

PASSES: XX

Format

SETTINGS: Off

To set the LBA to 1, go to ***LBAS*** then tap the edit icon and enter the value: 1



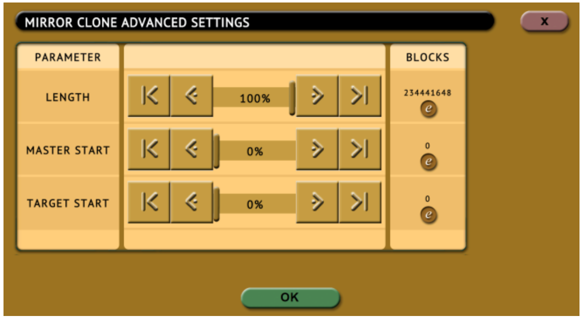
LBAS

0%

1

Start the wipe task. The task should finish quickly as it is resetting just wiping the HPA/DCO and 1 LBA.

Tap ***Mirror Settings*** and the following screen will appear:



MIRROR CLONE ADVANCED SETTINGS

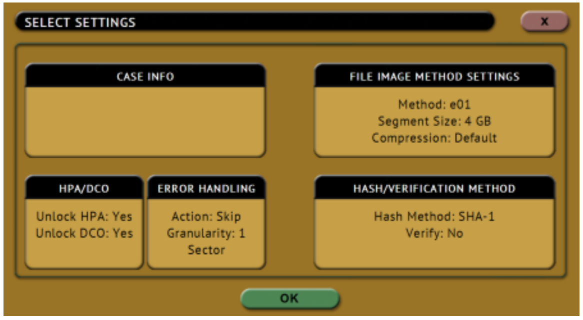
PARAMETER		BLOCKS
LENGTH	100%	234441648
MASTER START	0%	0
TARGET START	0%	0

- **Length –** Set the percentage or number of blocks to clone. For forensic purposes, this is typically set to 100% of the Source.
- **Master Start –** Set the percentage or number of blocks from the start of the Source (Master). For forensic purposes, this is typically set to 0%, or the beginning of the Source (Master).
- **Target Start** – Set the percentage or number of blocks from the start of the Destination (Target). For forensic purposes, this is typically set to 0%, or the beginning of the Destination (Target).

> Alternatively, the specific number of blocks can be set for each of the options by tapping the: e ***(edit)*** icon.

5.0.3.5.2 Special Settings for Drive to File

When ***Drive to File*** mode is selected, ***File Image Method Settings*** will appear on the top-right of the Settings screen:



SELECT SETTINGS

CASE INFO

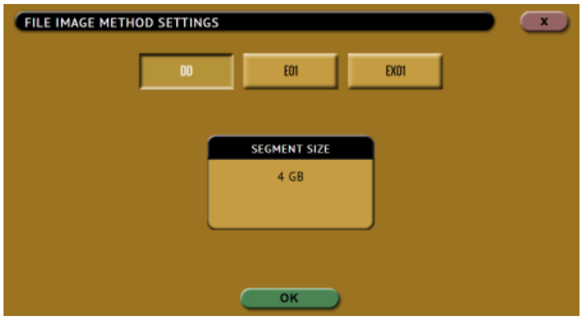
FILE IMAGE METHOD SETTINGS
Method: e01
Segment Size: 4 GB
Compression: Default

HPA/DCO
Unlock HPA: Yes
Unlock DCO: Yes

ERROR HANDLING
Action: Skip
Granularity: 1 Sector

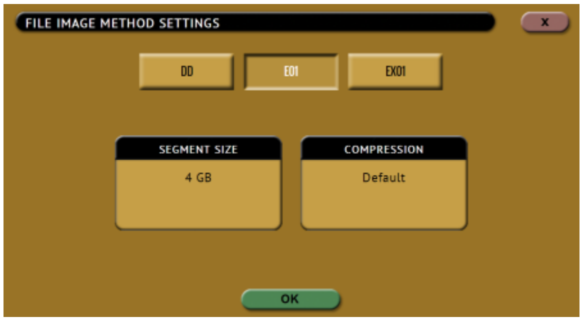
HASH/VERIFICATION METHOD
Hash Method: SHA-1
Verify: No

Tap ***File Image Method Settings*** and the following screen will appear when DD is selected:



SEGMENT SIZE
4 GB

The following screen will appear when E01 or EX01 is selected:



SEGMENT SIZE
4 GB

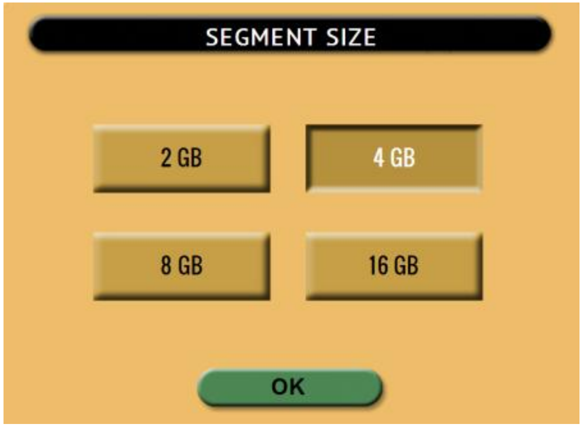
COMPRESSION
Default

One of three different images methods can be selected:

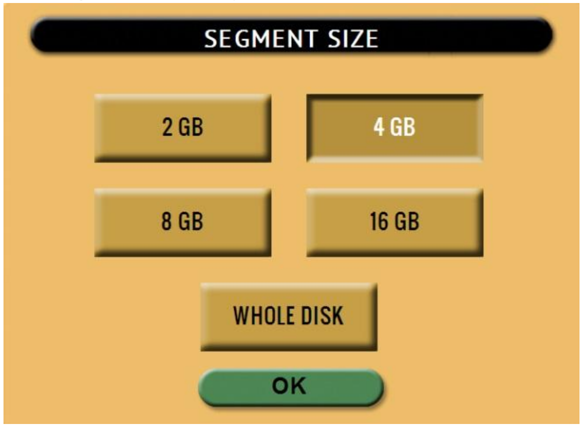
- **DD –** Uncompressed raw image files readable by many forensic programs.
- **E01 –** Compressed or uncompressed EnCase legacy evidence file format.
- **EX01 –** Compressed or uncompressed EnCase evidence file format.

SEGMENT SIZE – Available for DD, E01, and EX01. Allows the user to set the output segment size (file size). Choose from **2 GB**, **4 GB**, **8 GB**, **or 16 GB**. A **Whole Disk** option is available for DD only.

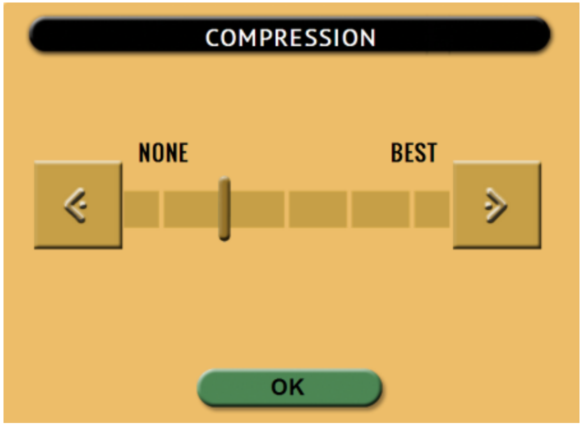
E01 and EX01 Segment Size options:



DD Segment Size Options:



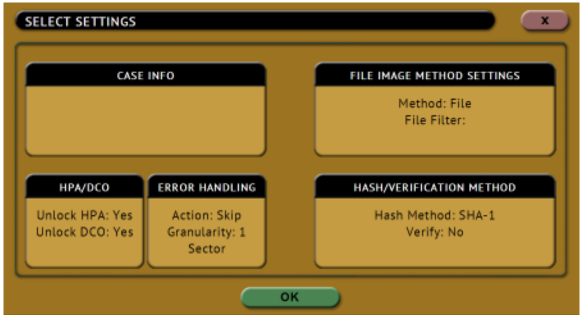
COMPRESSION – Available for E01 and EX01 only. Sets the compression level for E01 or EX01 imaging. When selecting Compression, the following screen will appear. Use the slider bar to adjust the desired compression level.



The higher the compression level, the longer it will take to image the Source drive. The ***Default*** compression setting (first setting, as seen in the picture above) is recommended when compression is used.

5.0.3.5.3 Special Settings for File to File

When File to File mode is selected, ***File Image Method Settings*** will appear on the top-right of the Settings screen:



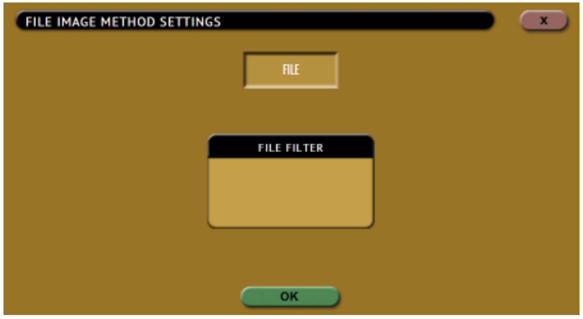
Method: File
File Filter:

Unlock HPA: Yes
Unlock DCO: Yes

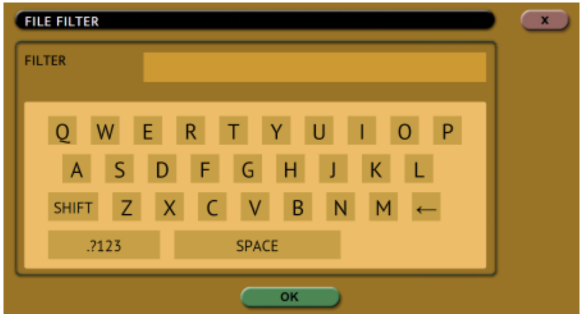
Action: Skip
Granularity: 1 Sector

Hash Method: SHA-1
Verify: No

Tap ***File Image Method Settings*** and the following screen will appear:



Tap ***File Filter*** to input the filter. Input the file extension filter desired, for example: ***.jpg***.



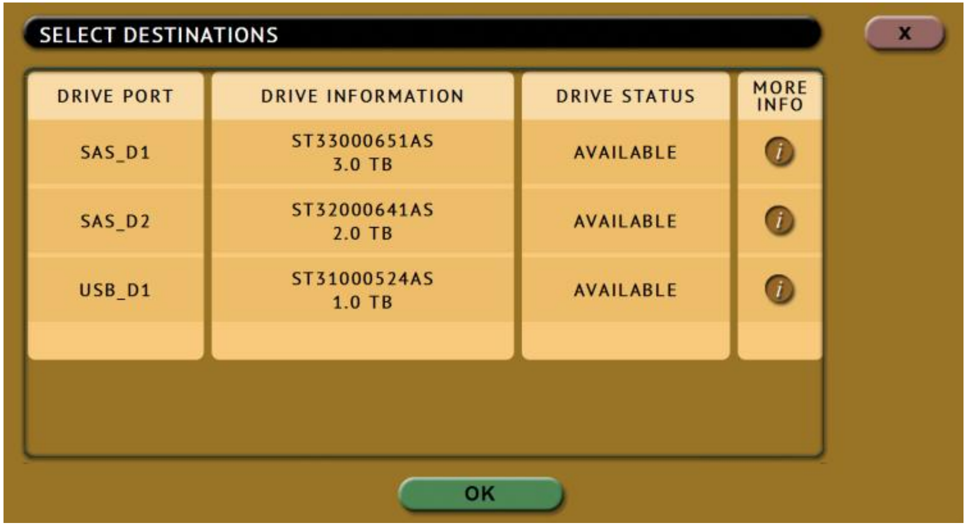
Multiple files can be specified by using a comma and no spaces, for example, ***.jpg,.zip,.mov,.mp3***

5.0.4 Destination / Image File

DESTINATION IMAGE FILE

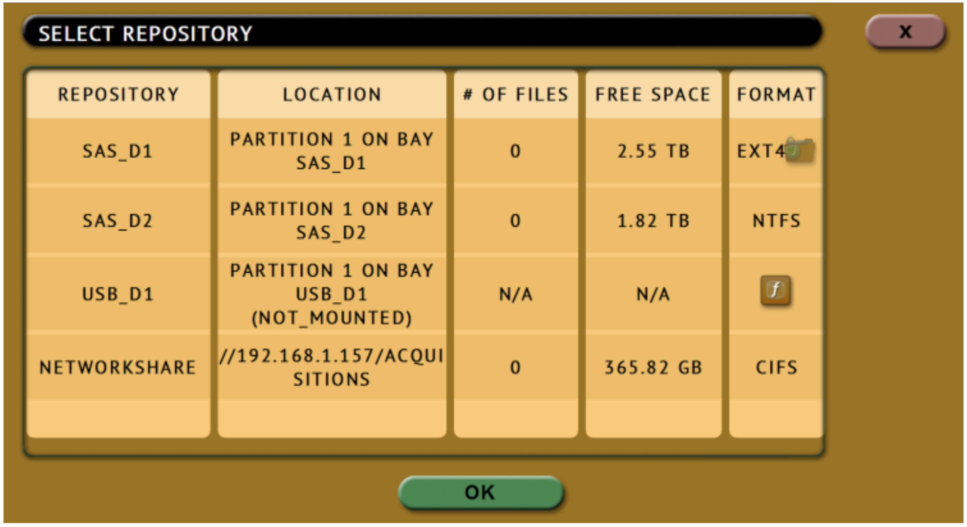
Tap the Destination or Image File icon to select the Destination drive or Image File. Falcon will list all the drives connected to the Destination position(s) and any repository configured as a Destination.

When ***Drive to Drive*** mode is selected, the Destination screen will show all drives connected to the Destination positions.



DRIVE PORT	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_D1	ST33000651AS 3.0 TB	AVAILABLE	ⓘ
SAS_D2	ST32000641AS 2.0 TB	AVAILABLE	ⓘ
USB_D1	ST31000524AS 1.0 TB	AVAILABLE	ⓘ

When ***Drive to File*** or ***File to File*** mode is selected, the Destination screen will show all drives connected to the Destination positions and any repository added with the Destination role (Destination or Both Source and Destination).



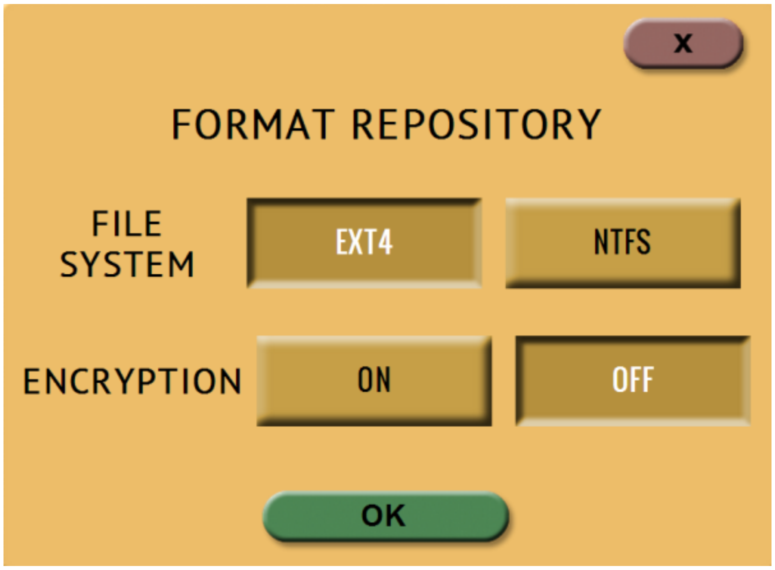
REPOSITORY	LOCATION	# OF FILES	FREE SPACE	FORMAT
SAS_D1	PARTITION 1 ON BAY SAS_D1	0	2.55 TB	EXT4
SAS_D2	PARTITION 1 ON BAY SAS_D2	0	1.82 TB	NTFS
USB_D1	PARTITION 1 ON BAY USB_D1 (NOT_MOUNTED)	N/A	N/A	f
NETWORKSHARE	//192.168.1.157/ACQUISITIONS	0	365.82 GB	CIFS

For DD, E01, Ex01, and File to File mode, the Falcon uses the EXT4 file system or NT file system (NTFS) to format drives. If the Destination drive is not formatted properly, the ***Location*** will appear as "***(NOT_MOUNTED)***" and a format icon will appear in the Format column. Tap the ***(Format)*** icon the Destination drive.

For Drive to File or File to File, the Falcon will display drives connected to the Destination ports and any added repository.

Encrypted drives will have the following symbol in the Format column:

When formatting the drive from this screen, a prompt will appear to format the drive.



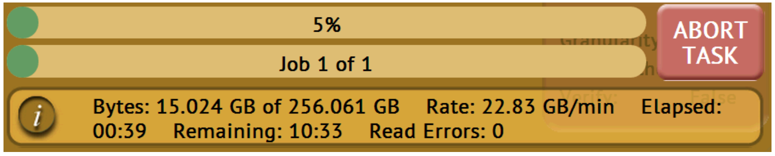
Select which file system to use (EXT4 or NTFS) and whether to format with encryption (ON) or without encryption (OFF). Details on encryption can be found in Chapter 8 of the Falcon User's Manual. For details on formatting a drive, see ***Section 6.0.3.2.3***. Formatting the drive may take up to two minutes. Tap the ***OK*** icon to continue.

For in-depth information regarding drive encryption, please see **Chapter 8: Drive Encryption and Decryption**

5.1 Starting the Imaging Operation

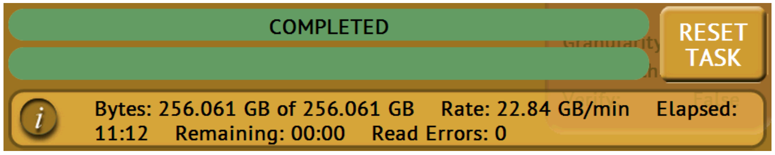
Once all the settings and options have been selected or set, tap the START ***(Start)*** icon to begin the imaging. A confirmation screen will appear. Tap the ***Yes*** icon to continue.

A progress bar will appear at the bottom of the screen showing the bytes processed, the rate (speed), elapsed time, and time remaining.



Bytes: 15.024 GB of 256.061 GB   Rate: 22.83 GB/min   Elapsed: 00:39   Remaining: 10:33   Read Errors: 0

When finished, the status will change to COMPLETED. At this point, it is recommended to tap Reset Task to reset the task, and also to delete the task in order for the drive bays to be properly reset and not show as being used or assigned for other tasks to be configured.



Bytes: 256.061 GB of 256.061 GB   Rate: 22.84 GB/min   Elapsed: 11:12   Remaining: 00:00   Read Errors: 0

The number of bytes shown on the progress bar is not the actual size of the drive. This is the actual data being processed. When 'Verify' is set to "Yes", the reported number will double in size.

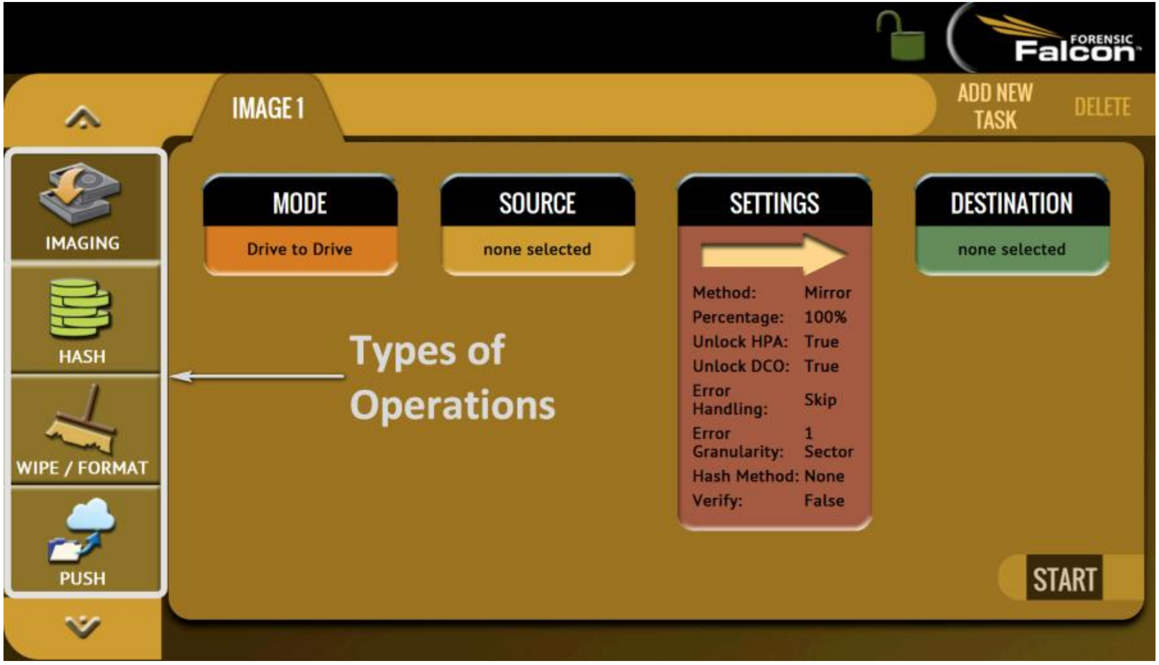
For parallel imaging, prior to starting the first task, users must set all other tasks that need to be run in parallel. When all other tasks to be run in parallel are set, a confirmation screen will appear stating there are multiple tasks setup with the same Source drive.

Falcon can automatically span to two (or more) Destination drives when using Drive to File mode (DD, E01, EX01). When the Destination drive is full and the remaining data to be imaged will not fit, Falcon will prompt for another drive. Information on Drive Spanning can be found in ***Section 3.1.1.1***.

6: Types of Operations

6.0 Types of Operations

There are thirteen (14) types of operation available on the Falcon. The left side of the screen shows the different operation types that can be set. Detailed information on all of the different operations and their screens can be found in this section.



MODE: Drive to Drive

SOURCE: none selected

SETTINGS:

Method:	Mirror
Percentage:	100%
Unlock HPA:	True
Unlock DCO:	True
Error Handling:	Skip
Error Granularity:	1 Sector
Hash Method:	None
Verify:	False

DESTINATION: none selected

Types of Operations

1. **IMAGING –** Performs an image from a Source to a Destination. There are three modes available:
    a. **Drive to Drive** – Performs a bit-for-bit copy of the Source producing an exact duplicate of the Source drive.
    b. **Drive to File** – Images the Source to any of the following image output formats: ***DD***, ***E01***, ***EX01***, or ***File***. Compression is available for E01 and EX01 formats.
    c. **File to File** – Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source and each file will be hashed.

    Details on the different screens found in the Imaging operation can be found in ***Chapter 5: Imaging***.
2. **HASH –** Perform a SHA1, SHA-256, or MD5 hash of a drive. This can also verify the hash of the drive by entering an “expected value” for the hash.

3. **WIPE –** This type of operation is used to erase, wipe, and/or format drives. There are three main settings:
    - **Secure Erase –** Sends a command to the drive instructing it to perform a secure erase based on the drive manufacturer's specifications.
    - **Wipe Patterns –** Allows the user to set a specific pattern to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set.
    - **Format –** Formats the Destination using the EXT4 file system or NT file system (NTFS) either with or without AES-256 encryption.
4. **PUSH –** The network Push feature gives users the ability to push evidence files from destination drives connected to the Falcon or from a Falcon repository to a network location. The Push feature provides a more secure method than simply copying and pasting to the analysis computer by performing an MD5 or SHA hash during the push process. Additionally users can select to verify the file transfer to ensure data integrity. Network users can then quickly preview data or copy data to a local drive or to any other directory on the network. The Falcon will create a log file for each push process.
5. **TASK MACRO –** Set up to nine (9) different tasks to perform sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe, image, hash, push, then wipe again.
6. **USB DEVICE –** Allows the user to view the contents of any drive connected to the Falcon from a computer connected via USB. When using this type of operation, all drives connected to the Falcon are write-protected.
7. **FILE BROWSER –** Preview the contents of all connected Source or Destination drives on the Falcon. The Falcon will show all viewable partitions and the contents of each partition.
8. **LOGS –** Display logs of each task that has been performed on the Falcon.
9. **STATISTICS –** This will display information about the Falcon including the current software installed. In addition, the Statistics screen has an ***Advanced Drive Statistics*** tab that shows raw S.M.A.R.T. data on any drive connected to the Falcon.
10. **MANAGE REPOSITORIES –** Allows the user to add a network location as a repository that can be used as a Destination for imaging or pushing images (or a Source when using the ***File to File*** mode).
11. **SYSTEM SETTINGS –** This mode allows changes to the system settings on the Falcon which include the following:
    - **User profiles/configurations –** Allows the user to create, save, apply, or delete user profiles/configurations.
    - **Passwords –** Allows the user to set a password to lock the Falcon from any configuration changes.
    - **Encryption Settings –** Sets the cipher mode (TC-XTS, CBC, or ECB), Cipher, IV Generation, and the encryption password.
    - **Language/Time Zone –** Sets the language on the Falcon's menu and change the system's Time Zone.
    - **Display –** Sets the Falcon's display/screen brightness and enable/disable Stealth Mode

12. **NETWORK SETTINGS –** Allows certain services to be enabled or disabled. Also, allows the user to set proxy settings (if required by their network).
13. **SOFTWARE UPDATES –** Perform software updates on the Falcon. Software can be updated over an internet connection (from network) or from a USB flash drive.
14. **POWER OFF –** Allows the user to turn the Falcon unit off by using the Graphical User Interface (GUI). Also allows a drive timeout to be set, powering down drives when not in use.

6.0.1 Imaging

This type of operation allows the imaging of a Source to a Destination. There are three different imaging modes and several settings to choose from. These selections should be performed in order from left to right.

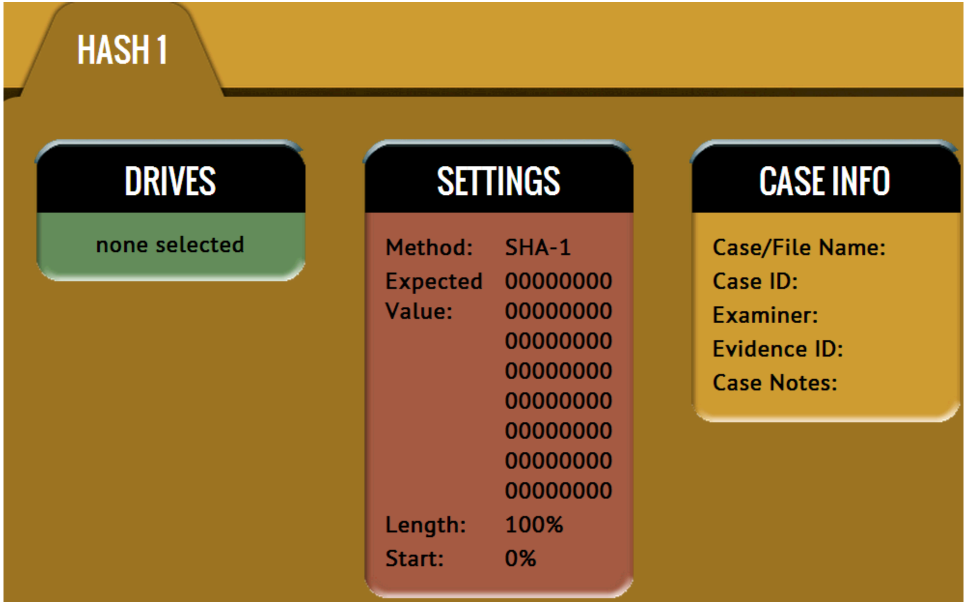
In-depth details on the different screens found in the Imaging operation can be found in **Chapter 5: Imaging**.

6.0.2 Hash

This type of operation allows the hashing of any connected drive using one of the following algorithms:

- SHA-1
- SHA-256
- MD5

There are three selections when performing a hash: ***Drives***, ***Settings***, and ***Case Info***.



none selected

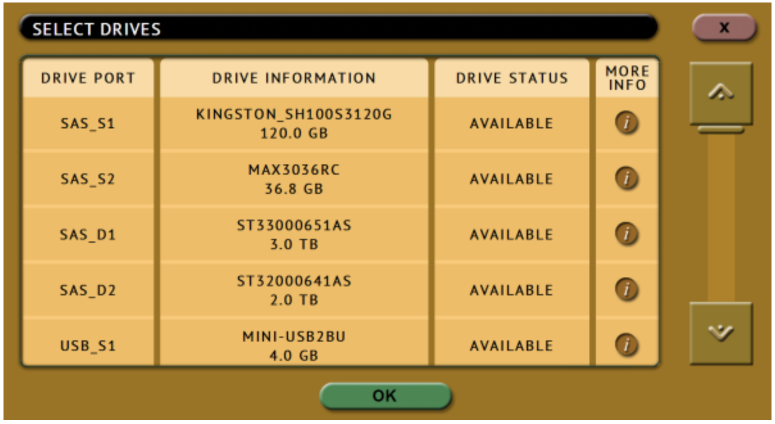
Method: SHA-1
Expected Value: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Length: 100%
Start: 0%

Case/File Name:
Case ID:
Examiner:
Evidence ID:
Case Notes:

6.0.2.1 Drives

DRIVES

Tap this icon to choose a drive to hash. Falcon will show all connected Source and Destination drives. Tap the drive to be hashed then tap ***OK***.



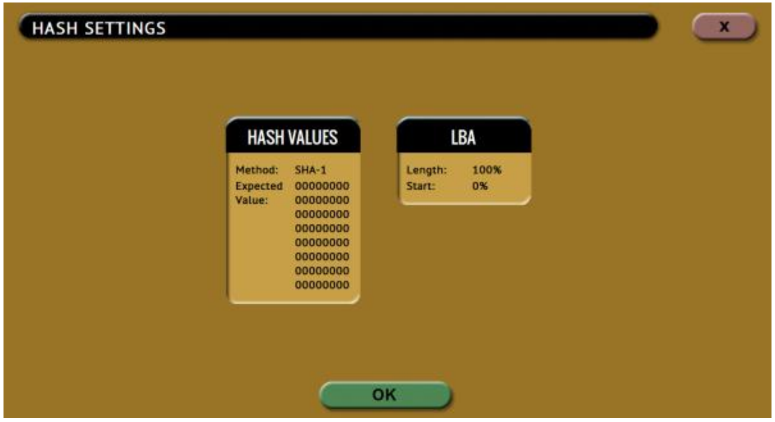
SELECT DRIVES

DRIVE PORT	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_S1	KINGSTON_SH100S3120G 120.0 GB	AVAILABLE	ⓘ
SAS_S2	MAX3036RC 36.8 GB	AVAILABLE	ⓘ
SAS_D1	ST33000651AS 3.0 TB	AVAILABLE	ⓘ
SAS_D2	ST32000641AS 2.0 TB	AVAILABLE	ⓘ
USB_S1	MINI-USB2BU 4.0 GB	AVAILABLE	ⓘ

6.0.2.2 Settings

SETTINGS

Tap this icon to choose a drive to adjust the hash settings. The Hash Settings screen will appear:



HASH SETTINGS

HASH VALUES

Method: SHA-1
Expected Value: 00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000

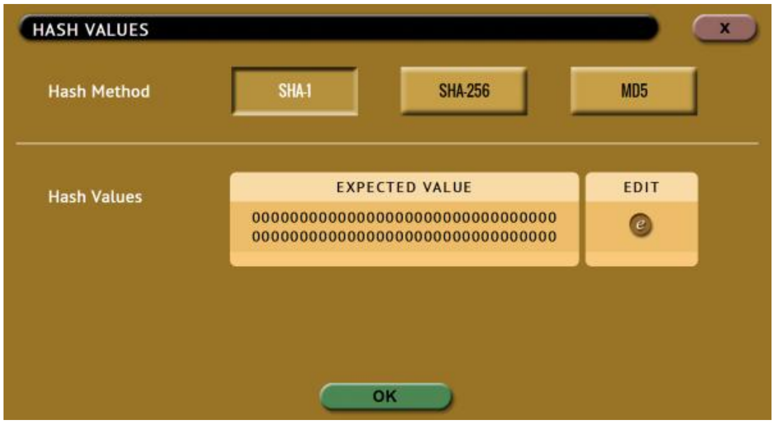
LBA

Length: 100%
Start: 0%

HASH VALUES

Tap this icon to set the hash method (SHA-1, SHA-256, or MD5) and to set the expected hash value (if desired). Setting the expected hash value instructs the Falcon to hash the drive then verify the hash with the expected value set.

> Each hash task is Logical Block Address (LBA) based and will hash drives based on the number of LBAs. If multiple drives are selected to be hashed, the Falcon will hash up to the LBA value of the smallest capacity drive. If drives with different capacities need to be hashed, it is recommended to start one task per drive.



```
0000000000000000000000000000000
0000000000000000000000000000000
```

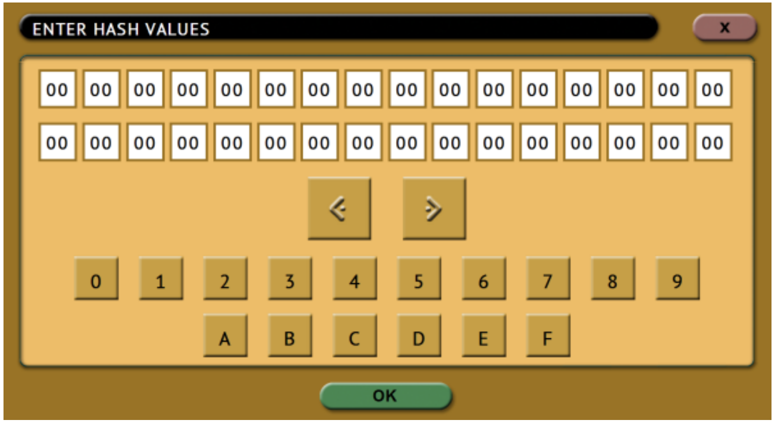
Hash Method Select one of the following hash methods:

- **SHA-1 –** Select this to hash or verify the Target drives using the SHA-1 algorithm.
- **SHA-256 –** Select this to hash or verify the Target drives using the SHA-256 algorithm.
- **MD5 –** Select this to verify the Target drives using the MD5 algorithm.

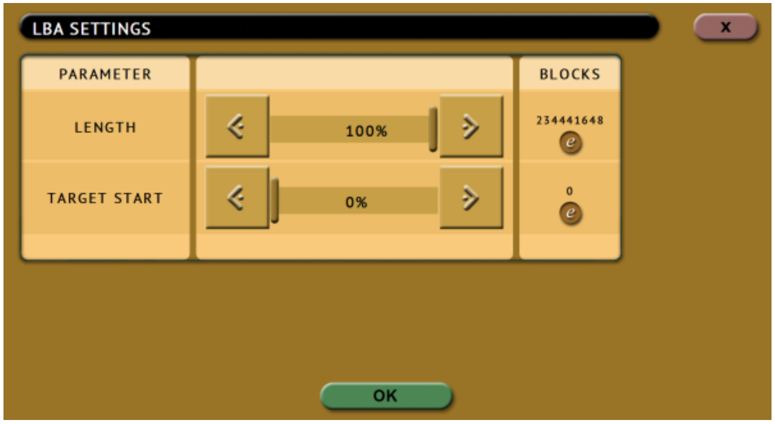
The recommended method is SHA-1 or SHA-256.

Hash Values By default, this value will have 0s (zeros). If this is not changed, or no value is entered, this will instruct the Falcon to hash the drive using the selected algorithm in the previous step. If a value is entered, the Falcon will hash the selected drive and verify hash with the value entered/edited.

To set the expected value, tap the ⓔ ***(edit)*** icon. The on screen keyboard will appear and the expected hash value can be set.



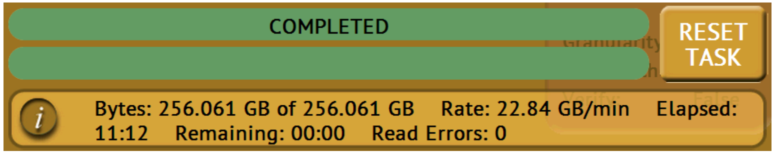
LBA The LBA icon will bring up the LBA settings screen. On this screen the user can adjust the percentage or the number of blocks of the drive to hash and also where to start the hash. By default the length is set to 100% (whole drive) and the starting percentage is set to 0% (start of the drive).



LBA SETTINGS

PARAMETER		BLOCKS
LENGTH	100%	234441648
TARGET START	0%	0

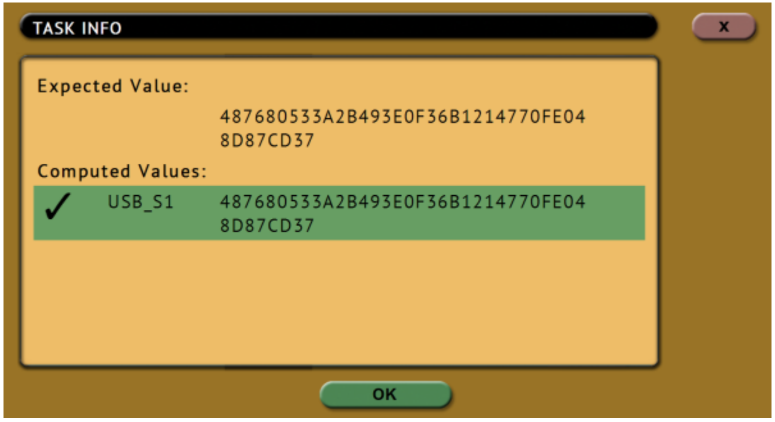
When the Falcon finishes hashing the drive, the following screen will appear showing the task completed.



COMPLETED

Bytes: 256.061 GB of 256.061 GB Rate: 22.84 GB/min Elapsed: 11:12 Remaining: 00:00 Read Errors: 0

Tap the ⓘ ***(Info)*** icon on the left of the completed screen to see both the expected hash value and the computed hash value.



TASK INFO

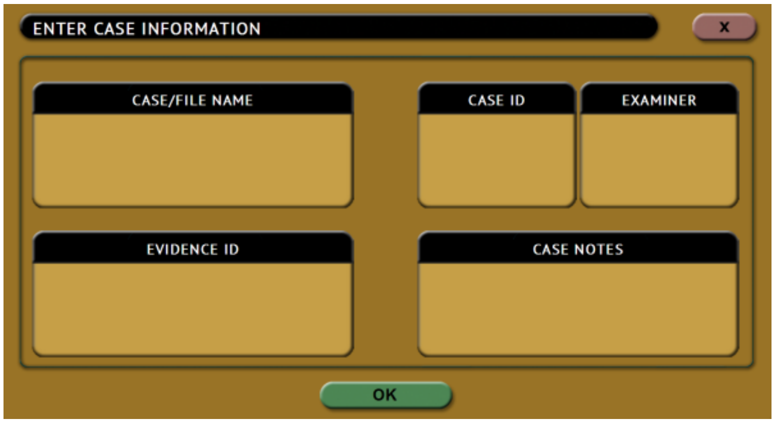
Expected Value:
487680533A2B493E0F36B1214770FE04
8D87CD37

Computed Values:
✓ USB_S1 487680533A2B493E0F36B1214770FE04
8D87CD37

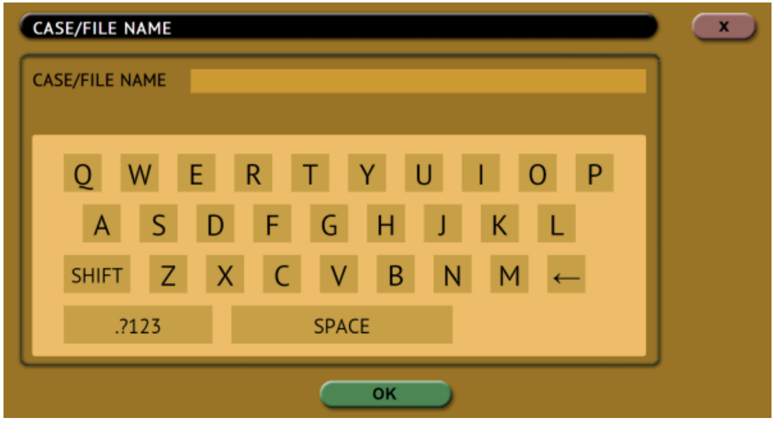
6.0.2.3 Case Info

CASE INFO The Case Info setting allows users to enter some information about the case. This is optional and is not required to start a Hash operation.

Information entered here will appear in the logs. More information on the Case Info screen can be found in ***Section 5.0.3.1***.



Tap any of the boxes and an on-screen keyboard will appear allowing information to be entered. After entering the information, tap the ***OK*** icon to go back to the previous screen.



The Falcon will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

Uppercase A to Z
Lowercase a to z
Numbers 0 to 9

Period (.)
Underscore (_)
Hyphen/Dash (-)

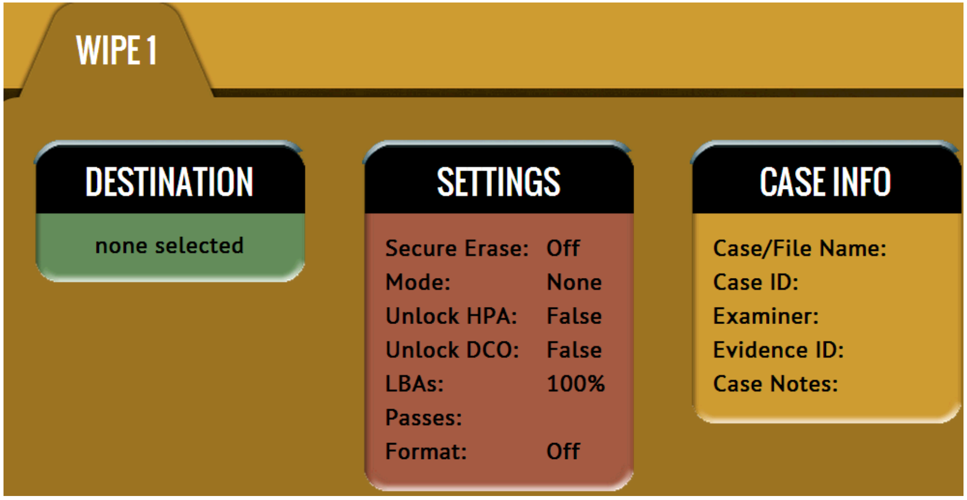
6.0.3 Wipe

This type of operation allows the user to erase, wipe, and/or format one or more Destination drives. There are three main settings: Secure Erase, Wipe Mode, and Format.

- **Secure Erase –** Sends a command to the drive instructing it to perform a secure erase based on the drive manufacturer's specifications for the secure erase command.
- **Wipe Patterns –** Allows the user to set a specific pattern to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set with pre-selected pass values.
- **Format –** Formats the Destination drive with an EXT4 file system or NT file system (NTFS) with or without AES-256 encryption.

More information on encryption can be found in ***Chapter 8***.

There are three selections when performing a wipe: ***Destination***, ***Settings***, and ***Case Info***.



none selected

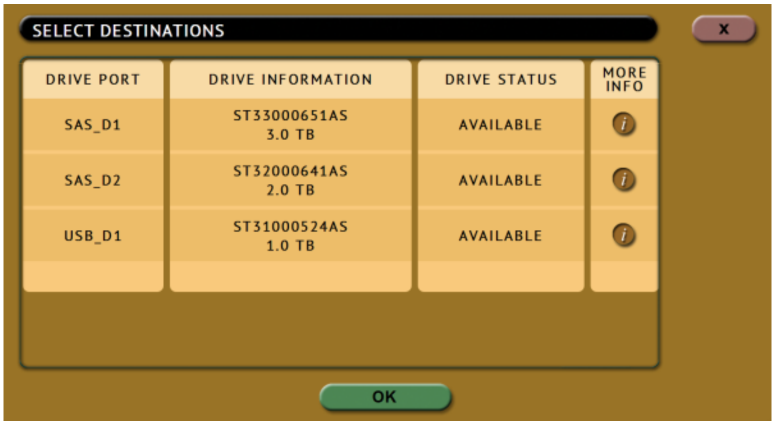
Secure Erase: Off
Mode: None
Unlock HPA: False
Unlock DCO: False
LBAs: 100%
Passes:
Format: Off

Case/File Name:
Case ID:
Examiner:
Evidence ID:
Case Notes:

6.0.3.1 Destination

DESTINATION Tap this icon to choose a drive to erase, wipe, and/or format.

A screen will appear, allowing the selection of one or more destinations. Tap the drive(s) to be erased, wiped, and/or formatted then tap ***OK***.



SELECT DESTINATIONS

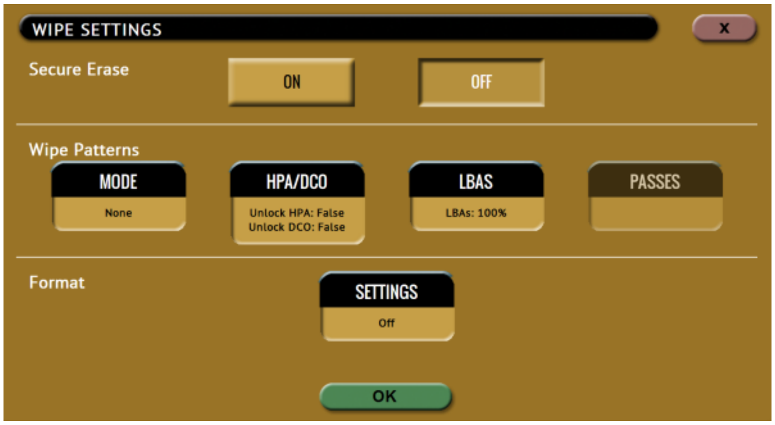
DRIVE PORT	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_D1	ST33000651AS 3.0 TB	AVAILABLE	ⓘ
SAS_D2	ST32000641AS 2.0 TB	AVAILABLE	ⓘ
USB_D1	ST31000524AS 1.0 TB	AVAILABLE	ⓘ

6.0.3.2 Settings

SETTINGS Tap this icon to choose a drive to set the wipe settings. The Wipe Settings screen will appear.

There are three sections in the ***Settings*** screen:

- Secure Erase
- Wipe Patterns
- Format



WIPE SETTINGS

Secure Erase: ON / OFF

Wipe Patterns:
MODE: None
HPA/DCO: Unlock HPA: False, Unlock DCO: False
LBAS: LBAs: 100%
PASSES

Format: SETTINGS: Off

The Falcon will perform each of the settings sequentially. For example, if Secure Erase is set to ON, a Wipe Pattern mode is specified, and Format is set to On, the Falcon will first secure erase the drive, then wipe the drive according to the mode specified, then format the drive.

6.0.3.2.1 Secure Erase

Secure Erase Choose ***ON*** to Secure Erase the selected Destination drive(s). Most drives support this function.

Secure Erase will send a command to the drive instructing it to reset itself to the specifications the drive manufacturer has set. For information on what happens when the Secure Erase command is sent, please contact the drive manufacturer. If the secure erase process fails, contact the drive manufacturer to find out if Secure Erase is supported on that specific drive.

For SAS (Serial Attached SCSI) drives, Secure Erase sends a 'Format' command. For SATA (Serial-ATA) drives, Secure Erase sends a 'Security Erase Unit' command. For SATA drives that support 'Enhanced Security Erase Unit' commands, the enhanced command will be sent. For questions on how each drive supports these features, or what the drive will do with these commands, please contact the drive manufacturer.

If errors appear when performing Secure Erase, contact the drive manufacturer to check if the drive supports Secure Erase. For Secure Erase specifications (what happens when the drive receives the Secure Erase command), contact the drive manufacturer.

6.0.3.2.2 Wipe Patterns

Wipe Patterns This setting allows the user to set a specific wipe pattern or patterns to use for wiping the drive. The number of passes is customizable (up to 7 passes) along with the type of data written for each pass. In addition, a 7-pass DoD wipe can be set with pre-selected pass values.

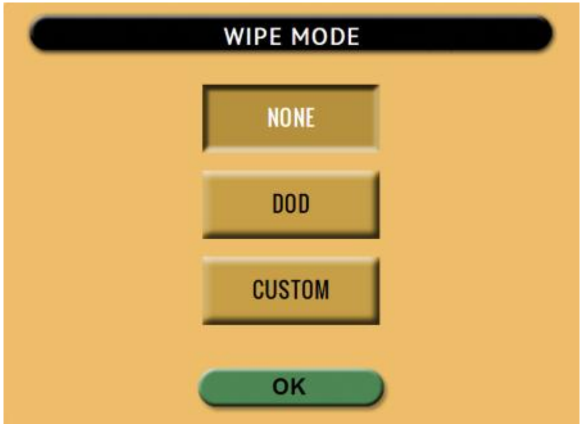
There are 4 selections when setting a wipe pattern:

- MODE
- HPA/DCO

- LBAS
- PASSES

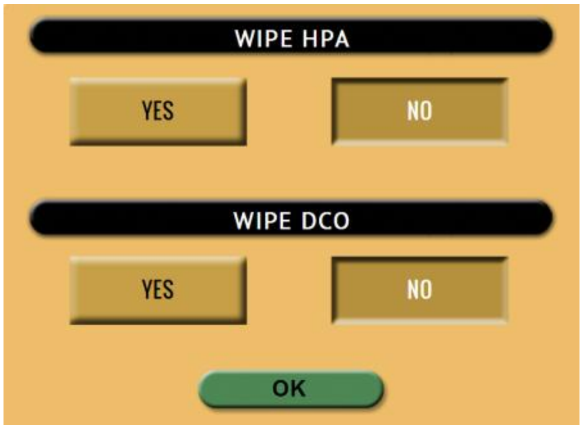
It is recommended to use the same capacity drive per task. When smaller capacity drives are wiped together with larger capacity drives, the smaller drives will finish first. However, the drive bays will not be available until the entire task is finished.

MODE Selecting this will open the Wipe Mode screen showing 3 options:



- **NONE –** Choosing this will instruct the Falcon not to perform a wipe using Wipe Mode.
- **DOD –** Choosing this will instruct the Falcon to perform a 7-pass wipe conforming to the DoD M-5220 standards.
- **CUSTOM –** Choosing this will allow the user to specify how many wipe passes will be performed and what values each pass will be written on each of the passes selected.

HPA/DCO This will open the HPA/DCO option for wiping. If the drive to be wiped has HPA and/or DCO that needs to be wiped, select ***Yes*** for the corresponding option.



LBA By default, this is set to 100% which will wipe all Logical Block Addresses (LBAs) and will wipe the entire drive (100%).

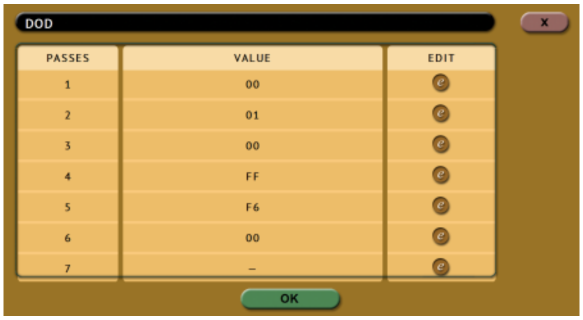
PASSES This Wipe Setting will change depending on the Wipe Pattern ***Mode*** selected.

- If ***None*** was selected, this is not selectable.

- If ***DoD*** was selected, the first six pass values will be filled automatically by default. It is mandatory that the user enter the 7th pass value by tapping the (edit) icon or the operation will fail.

- If ***Custom*** was selected, no passes will be filled out. It is mandatory that the user set the value for at least one pass or the wipe operation will fail. The pass value can be set by tapping the ⓔ ***(edit)*** icon.

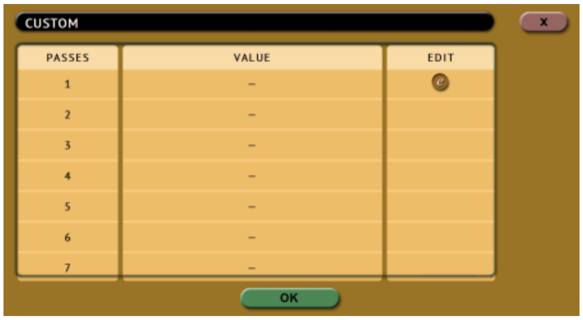
Passes screen when DOD is selected:


DOD

PASSES	VALUE	EDIT
1	00	ⓔ
2	01	ⓔ
3	00	ⓔ
4	FF	ⓔ
5	F6	ⓔ
6	00	ⓔ
7	–	ⓔ

The Falcon automatically enters default values for pass numbers 1 through 6. It is mandatory that the user enters a value for the 7th pass or the Falcon will not proceed with the wipe operation. Values can be changed or added by tapping the ⓔ ***(edit)*** icon.

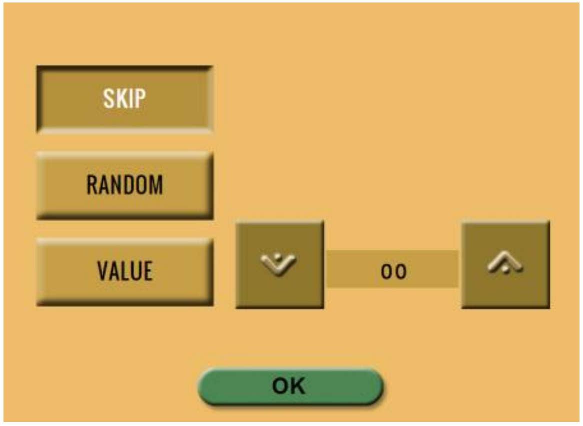
Passes screen when Custom is selected:



PASSES	VALUE	EDIT
1	–	ⓔ
2	–	
3	–	
4	–	
5	–	
6	–	
7	–	

There is no default value entered for any passes. It is mandatory that the user select a value for at least the first pass or the Falcon will not proceed with the wipe operation. Values can be changed or added by tapping the ⓔ ***(edit)*** icon.

Editing one or more of the passes in DOD or CUSTOM mode will bring up this screen:



- **SKIP –** Instructs the Falcon to skip the pass.
- **RANDOM –** Instructs the Falcon to perform a random pattern or value.
- **VALUE –** Instructs the Falcon to use the specified hex value to be written for the pass. The values can range anywhere from 00 to FF.

6.0.3.2.3 Format

Format

Formats the Destination using the EXT4 file system or NT file system (NTFS) either with or without AES-256 encryption. To format the drive (with or without encryption) tap the ***Settings*** icon.

> ⚠ The Falcon will check the Destination drive for proper formatting prior to being used as a Destination or Repository for Imaging using ***Drive to File*** or ***File to File***. If it is not properly formatted, Destination drive must be formatted using the Falcon prior to being used as a Destination or Repository for Imaging using ***Drive to File*** or ***File to File***.

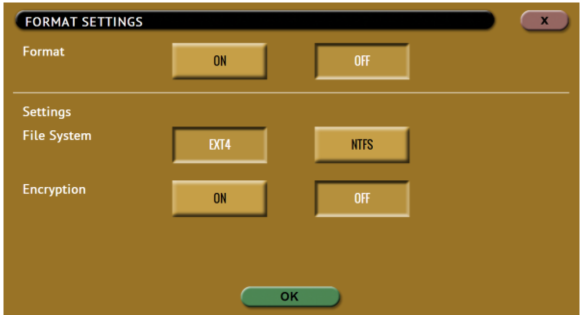
SETTINGS

Tap this icon to set the Falcon to format the drive (with or without encryption). Three settings are available:

- **Format –** When set to ***ON***, the Falcon will format the Destination drive with or without encryption. The drive will be formatted with the EXT4 file system or NT file system (NTFS), depending on which file system is chosen. When set to ***OFF***, the Falcon will not format or encrypt the selected drive.
- **File System –** Select ***EXT4*** to format the Destination using the EXT4 file system.

Select ***NTFS*** to format using the NT file system (NTFS).

- **Encryption –** Select ***ON*** to format the drive with encryption. The drive will be formatted with the EXT4 file system or NT file system (NTFS) and encrypted with the AES-256 algorithm.



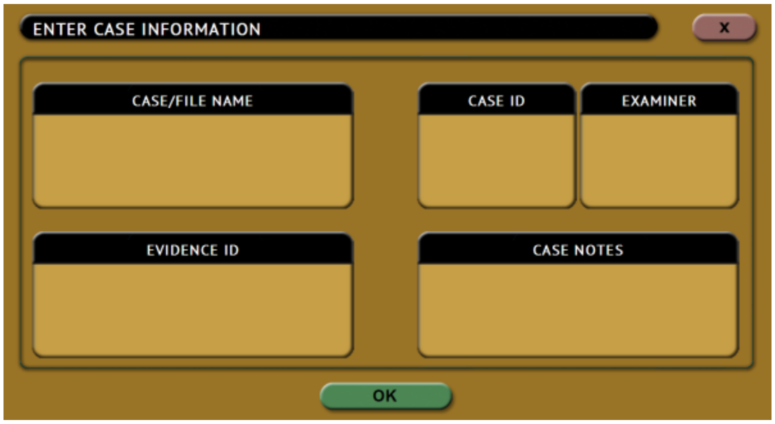
For more information on encrypted Destination drives, please see **Chapter 8: Drive Encryption and Decryption**.

6.0.3.3 Case Info

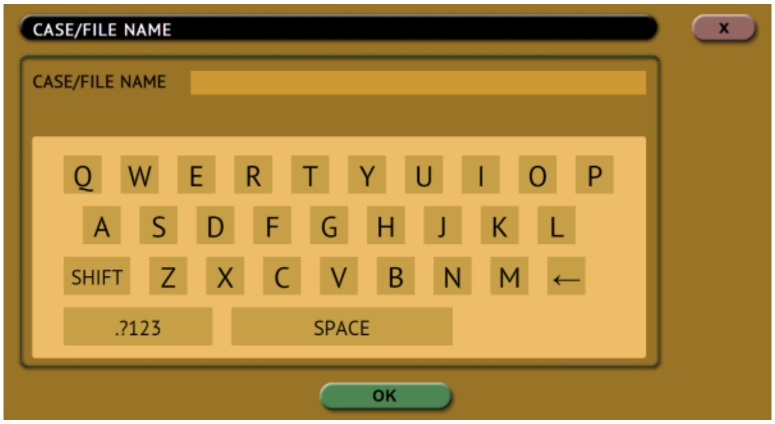
CASE INFO

The Case Info setting allows users to enter some information about the case. This is optional and is not required to start a Wipe operation.

Information entered here will appear in the logs. More information on the Case Info screen can be found in ***Section 5.0.3.1***.



Tap any of the boxes and an on-screen keyboard will appear allowing information to be entered. After entering the information, tap the ***OK*** icon to go back to the previous screen.



The Falcon will convert any non-POSIX portable characters used in ***Case/File Name*** field to underscores "_" when creating the log or file names.

POSIX portable characters are:

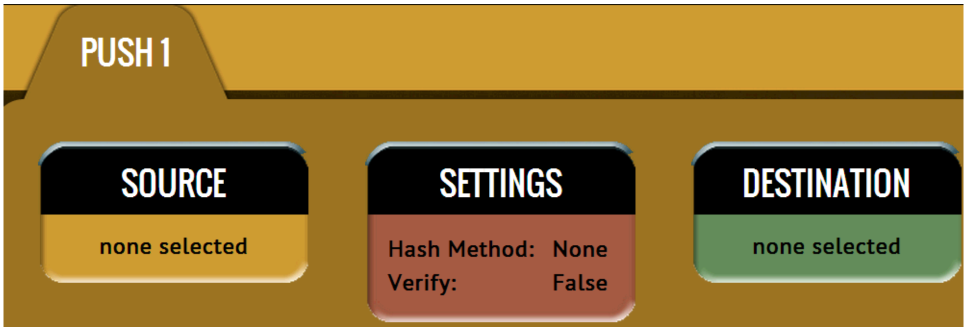
Uppercase A to Z	Period (.)
Lowercase a to z	Underscore (_)
Numbers 0 to 9	Hyphen/Dash (-)

6.0.4 Push

The network Push feature gives users the ability to push evidence files from destination drives connected to the Falcon or from a Falcon repository to a network location or a Destination drive connected to the Falcon. The Push feature provides a more secure method than simply copying and pasting to the analysis computer by performing an MD5 or SHA hash during the push process. Users can also select to verify the file transfer to ensure data integrity. The Falcon will create a log file for each push process.

There are three selections when performing a push:

- Source
- Settings
- Destination



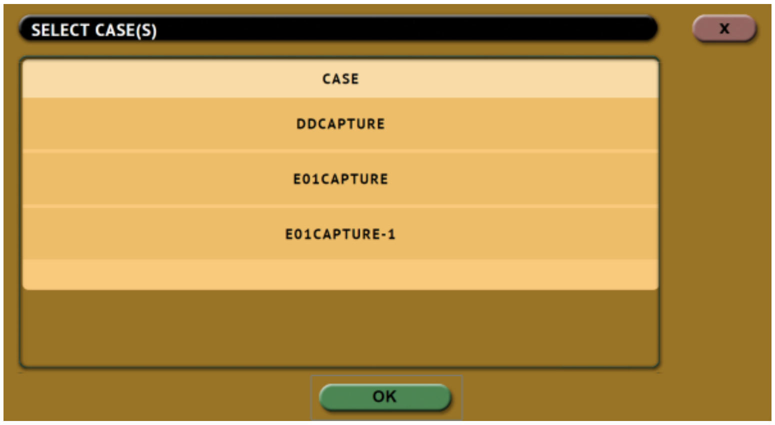
To push files to a network location, a network repository must be set up. Details on how to add a repository can be found in ***Section 6.0.10.1***.

6.0.4.1 Source

SOURCE

Tap this icon to select the drive or repository where the files are to be pushed from (where the files to push are located). This will only show drives connected to the Destination ports or locations set up as a repository where the DD, E01, or EX01 images are located.

After selecting the Source, a list of cases found on the drive will be displayed. Select one or more cases to push then tap the ***OK*** button to continue. If no cases are selected, all cases found on the drive or repository will be pushed.



CASE
DDCAPTURE
E01CAPTURE
E01CAPTURE-1

6.0.4.2 Settings

SETTINGS

(Optional) Tap this icon to enter case info, set a hash method, and to set the verify option. The case info screen is similar to previous case info screens.

There are four hash methods available for this operation:

- **None –** No hash will be performed.
- **SHA-1 –** The SHA-1 algorithm will be performed on each file from the source location.
- **MD5 –** The MD5 algorithm will be performed on each file from the source location.

SHA-1 is the recommended method.

There are two verify settings available:

- **Yes –** Each file that was copied (on the Destination location) will be verified using the selected hash method/algorithm selected.
- **No –** No verification will be made.

6.0.4.3 Destination

DESTINATION

Tap this icon to select the drive or repository where the files are to be pushed to (where the files to push will be pushed/copied to). This will only show drives connected to the Destination ports or locations set up as a repository where the DD, E01, or EX01 images will be pushed to.

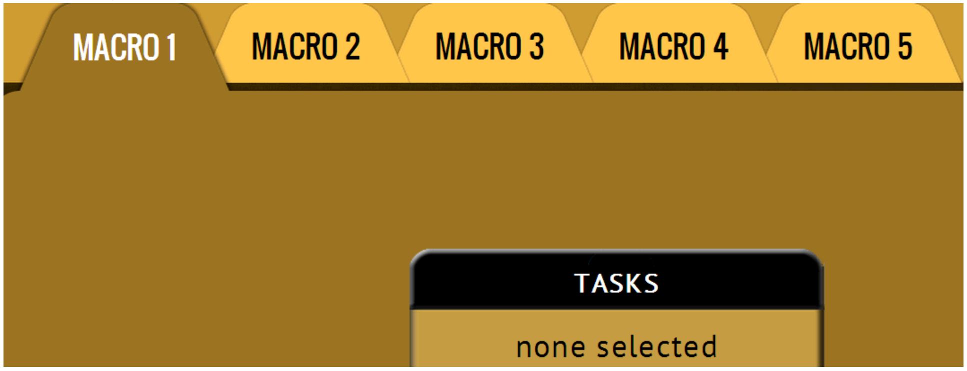
6.0.5 Task Macro

1. dd
2. Hash
3. Wipe

TASK MACRO

This operation allows up to five (5) macros that can be set. Each macro can run up to nine (9) tasks sequentially (one after another). For example, a macro can be set to perform these tasks in order: Wipe, image, hash, push, then wipe again.

Each of the five macros can be set by tapping on the Macro number as seen in the next picture:



TASKS

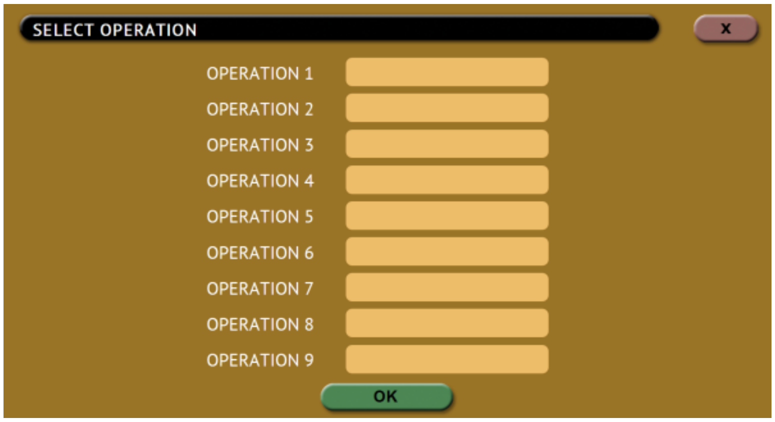
none selected

Each task or operation must be set up before setting up the macro. For example, to set up a Task Macro that will perform a wipe, then image, users must first set up both the wipe and image tasks. Once the wipe (for example, Wipe 1) and image (for example, Image 1) has been set up, the Task Macro can be set.

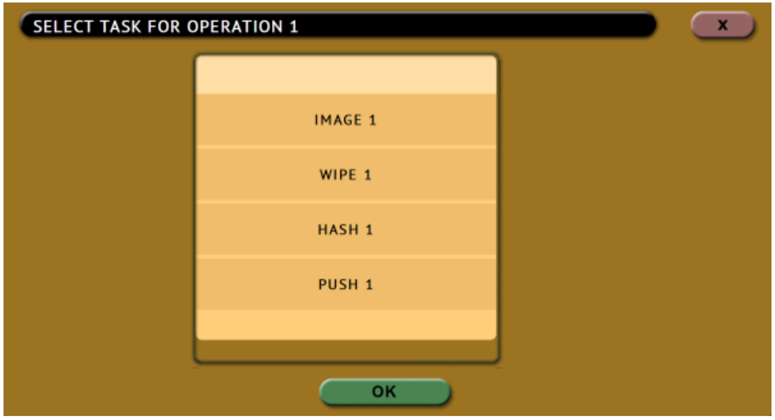
6.0.5.1 Tasks

TASKS

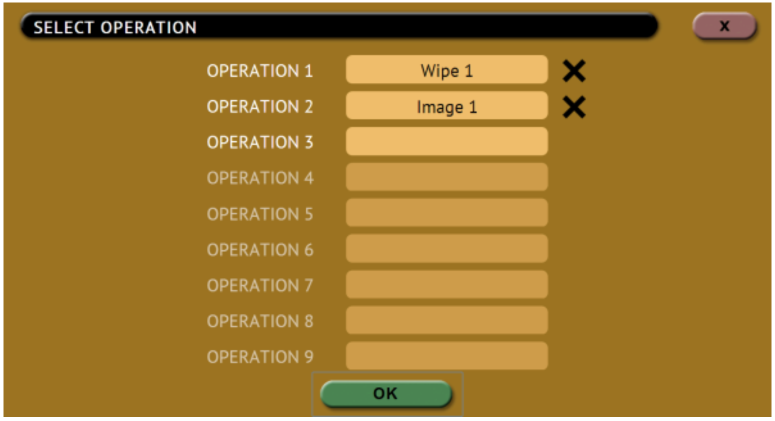
Tapping this icon allows the user to set specific tasks for each macro. The following window will appear:



Tap ***Operation 1*** to set the first operation in the macro. The following screen will appear allowing the user to choose the task. Tap the ***OK*** icon to continue.



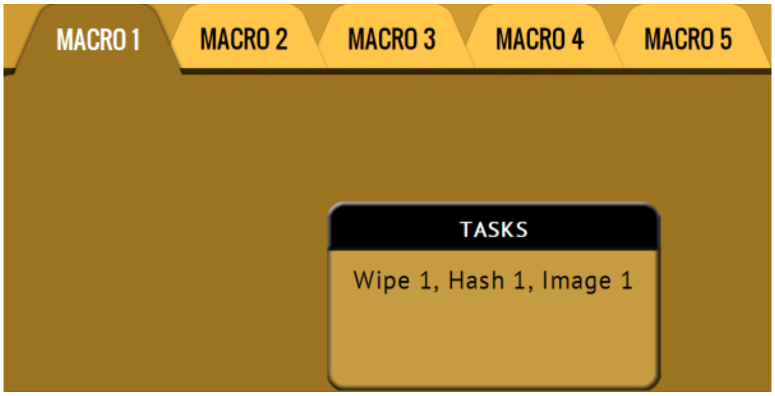
Continue adding operations desired. Each operation added will appear on the list. To delete an operation, tap the ***X*** to the right of the operation.



OPERATION 1 Wipe 1 ✕

OPERATION 2 Image 1 ✕

When finished, tap the ***OK*** icon. A summary of the macro will be seen:



TASKS

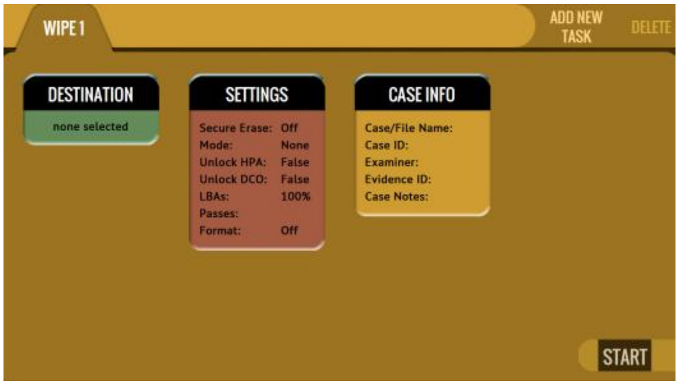
Wipe 1, Hash 1, Image 1

To start the macro and have the Falcon perform all the operations on the task list, tap the ***Start*** icon.

Example: Setting up a Macro for a Wipe using Secure Erase then perform a Drive to Drive Image

To set a macro to perform a Wipe using Secure Erase on SAS_D1, immediately followed by performing a Drive to Drive image from SAS_S1 to the newly wiped (secure erased) SAS_D1, the Wipe and Imaging Tasks first need to be set up.

1. First, set the Wipe task. Select SAS_D1 as the Destination and change the setting to perform a Secure Erase (Wipe Patterns and Format set to off). Do not start this task.



DESTINATION

none selected

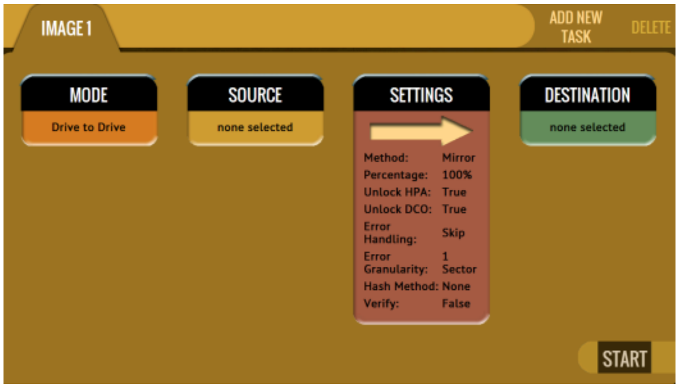
SETTINGS

Secure Erase: Off
Mode: None
Unlock HPA: False
Unlock DCO: False
LBAs: 100%
Passes:
Format: Off

CASE INFO

Case/File Name:
Case ID:
Examiner:
Evidence ID:
Case Notes:

2. Next, set the Imaging task. Select Drive to Drive as the Mode. Select SAS_S1 as the Source. Change the settings as needed. Select SAS_D1 as the Destination. Do not start this task.



MODE: Drive to Drive

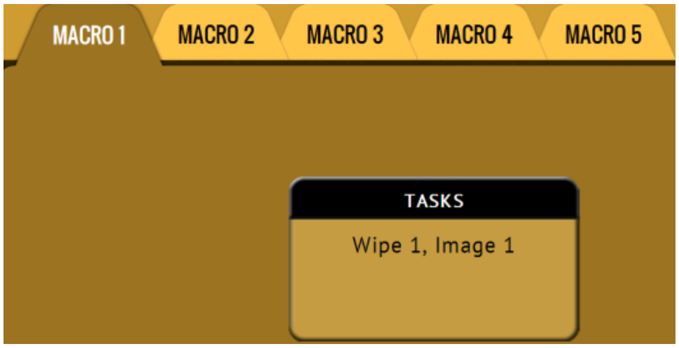
SOURCE: none selected

SETTINGS

Method:	Mirror
Percentage:	100%
Unlock HPA:	True
Unlock DCO:	True
Error Handling:	Skip
Error Granularity:	1 Sector
Hash Method:	None
Verify:	False

DESTINATION: none selected

3. Choose ***Task Macro*** from the list of operations on the left side.
4. Tap the ***Tasks*** icon to select the different tasks for the macro.
5. Tap the field next to ***Operation 1*** to set the first operation. Since the first task to be run is the Wipe task, select ***Wipe 1*** then tap ***OK***.
6. Tap the field next to ***Operation 2*** to set the second operation. Since the second task to be run is the Drive to Drive Imaging task, select ***Image 1*** then tap ***OK***.
7. The screen should now show ***Wipe 1, Image 1*** as the Tasks for Macro 1.

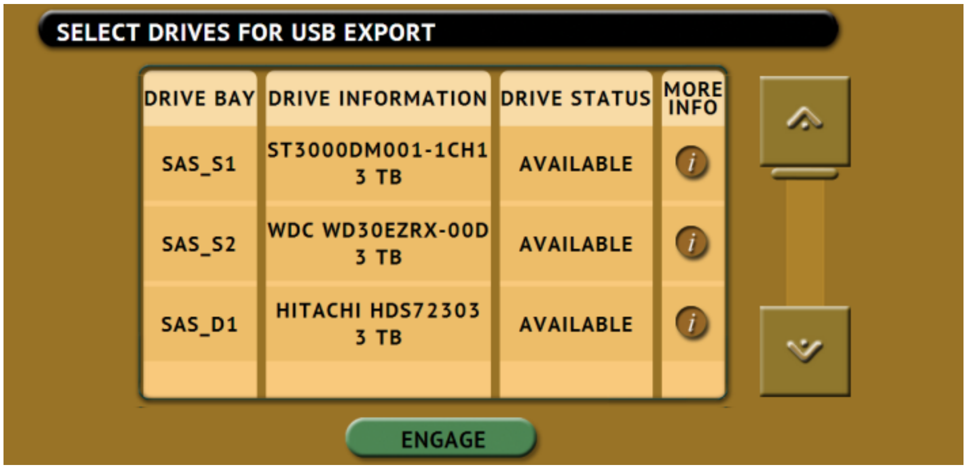


TASKS: Wipe 1, Image 1

8. Tap the ***Start*** icon to begin the macro. The macro will run the Wipe 1 task first, then Image 1.

6.0.6 USB Device

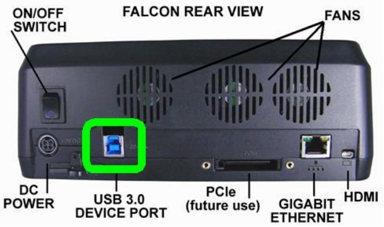
Connecting the Falcon to a computer via USB will allow the user to view any drive connected to the Falcon. In this mode, all drives connected to the Falcon are write-protected. When this type of operating is selected, the following screen will appear:



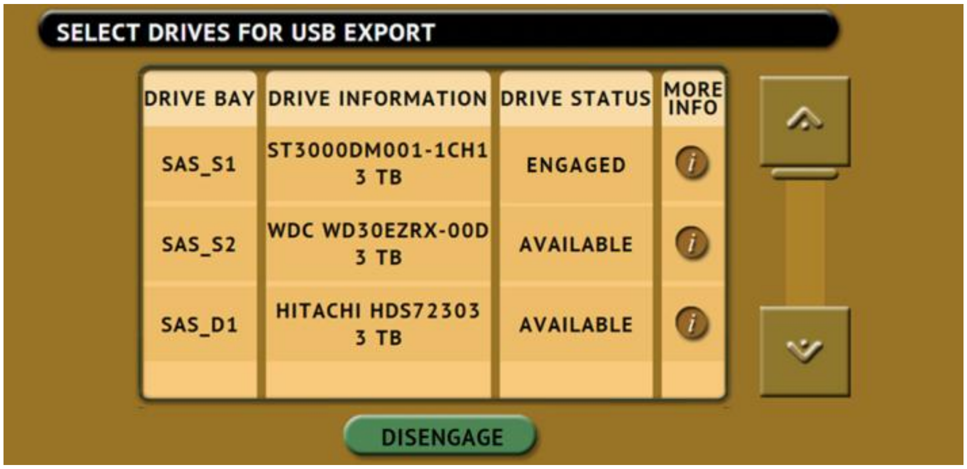
SELECT DRIVES FOR USB EXPORT

DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_S1	ST3000DM001-1CH1 3 TB	AVAILABLE	ⓘ
SAS_S2	WDC WD30EZRX-00D 3 TB	AVAILABLE	ⓘ
SAS_D1	HITACHI HDS72303 3 TB	AVAILABLE	ⓘ

When using this type of operation, use the **USB Device port** located on the back panel of the Falcon.



Choose the drive to view then tap the ***ENGAGE*** icon. The 'DRIVE STATUS' for the selected drive will change to "ENGAGED" and the ***ENGAGE*** icon will change to ***DISENGAGE***. At this point, connect a USB cable between the computer and the Falcon.



SELECT DRIVES FOR USB EXPORT

DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_S1	ST3000DM001-1CH1 3 TB	ENGAGED	ⓘ
SAS_S2	WDC WD30EZRX-00D 3 TB	AVAILABLE	ⓘ
SAS_D1	HITACHI HDS72303 3 TB	AVAILABLE	ⓘ

Connect a USB cable (A Male to B Male USB cable, one was included with the Falcon) between the computer and the Falcon. Connect the USB B connector to the Falcon's USB Device Port located on the back panel of the Falcon. Connect the USB A connector to an available USB port on the computer.

After a few moments, Windows should assign a drive letter to the selected drive. The contents of the drive should now be accessible in Windows.

When finished, tap the ***DISENGAGE*** icon to disengage the USB mode. The USB cable can now be disconnected from the computer and the Falcon.

Only one drive can be engaged at a time.

6.0.7 File Browser

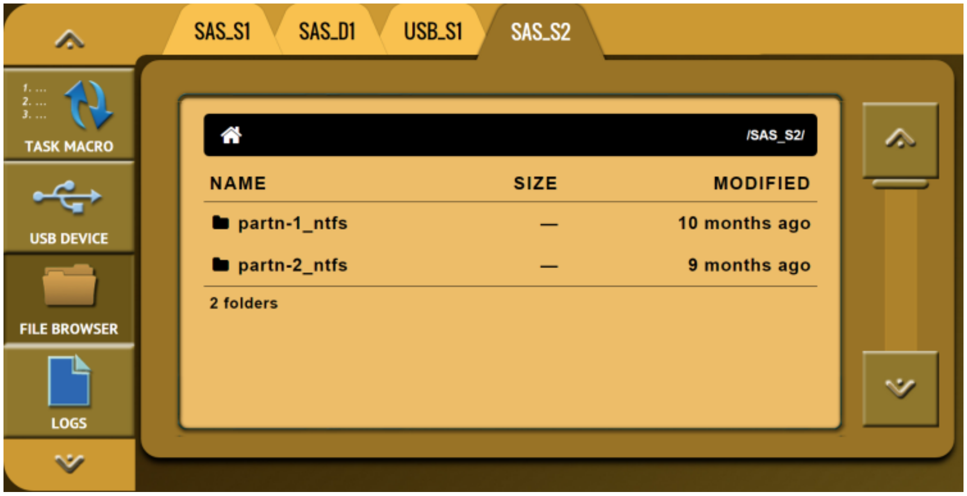
The contents of all connected Source or Destination drives on the Falcon can be viewed using the Falcon's file browser. The Falcon will show the partitions and the contents of each partition. Note that only some files can be opened by the Falcon.

For Destination drives, only drives formatted by the Falcon can be previewed. Contents of Destination drives that were used in a 'Drive to Drive' image will not be seen.

Drives connected to the Source ports (SAS_S1, SAS_S2, USB_S1, and FW_S1) – Drives connected to the Source ports are always write-protected. Using the File Browser function will not alter the drive or its contents in any way.

Drives connected to the Destination ports (SAS_D1, SAS_D2, USB_D1, and USB_D2) – Drives connected to the Destination ports are not write-protected. The File Browser function only opens a file and does not modify the contents of the file. The only change to the contents of the destination drive will be the file's accessed date and time.

In the File Browser screen, select the drive to view:

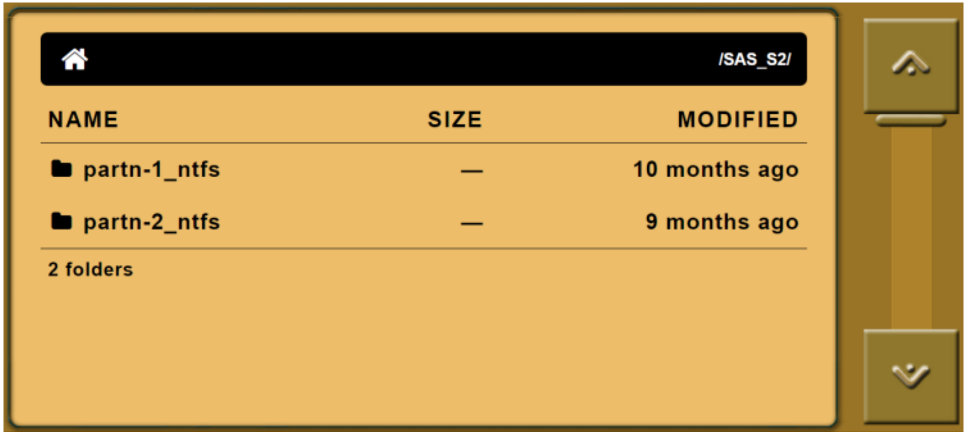


/SAS_S2/

NAME	SIZE	MODIFIED
partn-1_ntfs	—	10 months ago
partn-2_ntfs	—	9 months ago

2 folders

Select the partition to view:

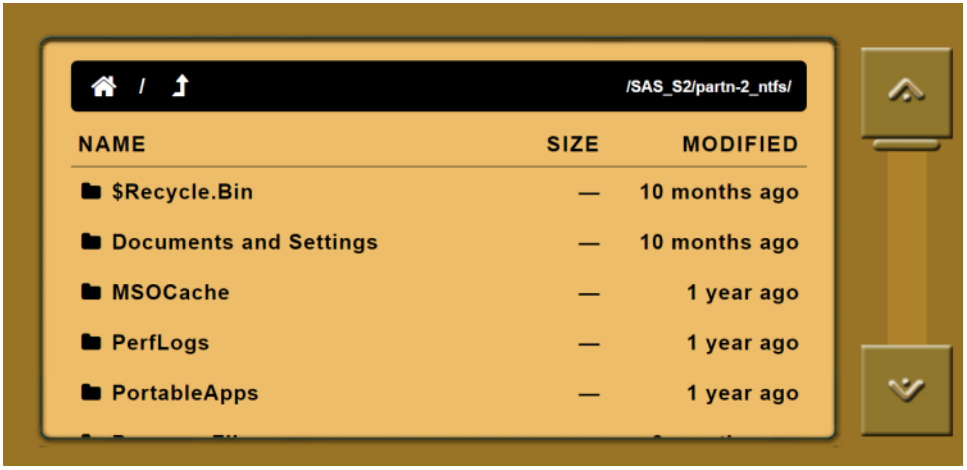


/SAS_S2/

NAME	SIZE	MODIFIED
partn-1_ntfs	—	10 months ago
partn-2_ntfs	—	9 months ago

2 folders

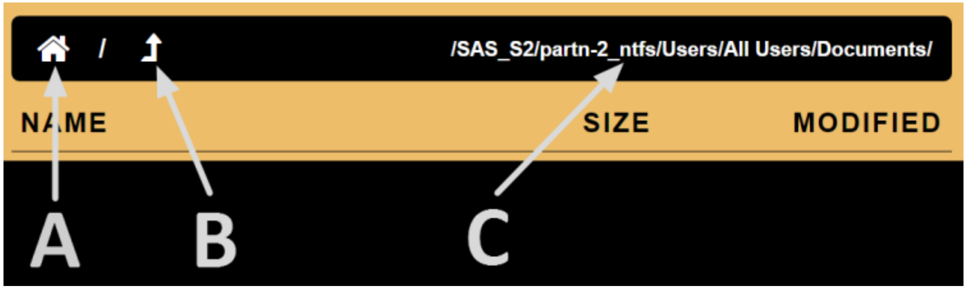
The folders/directories and files in that partition will be displayed:



/SAS_S2/partn-2_ntfs/

NAME	SIZE	MODIFIED
$Recycle.Bin	—	10 months ago
Documents and Settings	—	10 months ago
MSOCache	—	1 year ago
PerfLogs	—	1 year ago
PortableApps	—	1 year ago

Legend:



/SAS_S2/partn-2_ntfs/Users/All Users/Documents/

NAME	SIZE	MODIFIED

A – Home – Tap the Home icon to bring you to the top-level of the drive.

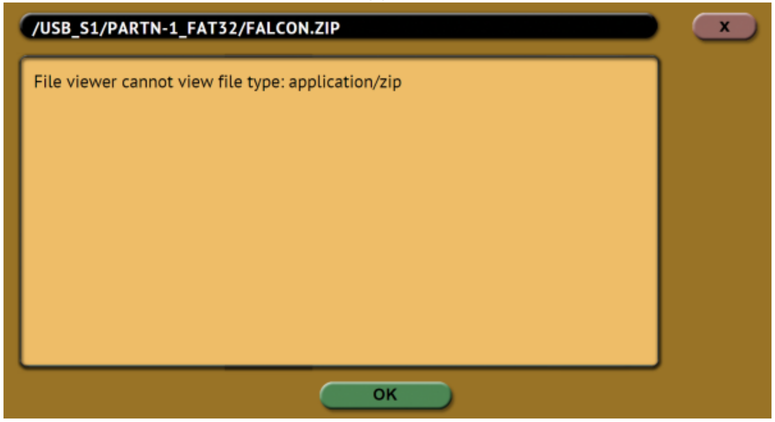
B – Up One Level – Tap this icon to go up one level (one folder/directory).

C – Path – Displays the current path to the folder/directory being viewed.

Falcon can open and preview certain files. Some of the files it can preview are:

*.jpg	*.txt
*.gif	*.pdf
*.png	*.html

If the Falcon cannot preview a file, a message will appear stating "**File viewer cannot view file type:**"



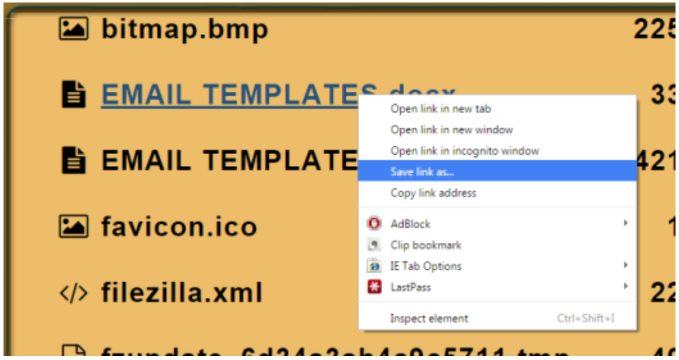
/USB_S1/PARTN-1_FAT32/FALCON.ZIP

File viewer cannot view file type: application/zip

6.0.7.1 Viewing files from the web interface

The Falcon's File Browser can also be used from the web interface. Using the web interface gives the ability to open files that the Falcon cannot preview by downloading the file to a computer (where the Falcon is being browsed from).

1. Using a compatible web browser, connect to the Falcon's web interface (see ***Section 10.1*** for more information on how to connect to the Falcon's web interface).
2. From the Falcon's web interface, navigate to ***File Browser***.
3. Select the drive to view.
4. Navigate through the file browser and locate the file to download and open.
5. From the File Browser screen, right-click on the file and select ***"Save link as…"*** and save the file to the local computer.



6. The file can then be opened on the computer where it was downloaded to.

Your computer will need to be able to open the type of file that was downloaded. For example, if a Word document was downloaded, the computer needs to have software that can open a Word document.

6.0.7.2 Important notes about using the File Browser

When using the Falcon's File Browser, there are several things to take note of:

- Drives connected to the Source positions are write-protected.
- When using the Falcon on-screen GUI, opening a file will not alter the forensic integrity of the Source drive connected to the Falcon.
- When using the web interface, opening a file or saving a file to a computer will not alter the forensic integrity of the Source drive connected to the Falcon.
- The Falcon file browser is not able to open every file to preview. When a file cannot be opened directly on the Falcon, the file can be saved on a computer by connecting to the Falcon's web interface (see ***Section 6.0.7.1*** for more information on viewing files from the web interface).

6.0.8 Logs

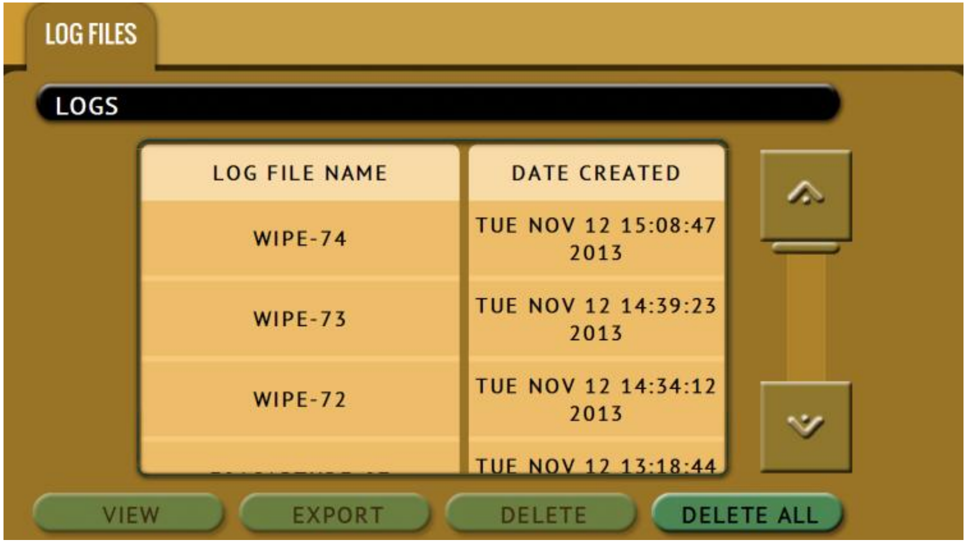
The Falcon keeps logs of all imaging, hash, wipe, format, and push operations. Logs can be viewed directly on the Falcon or from a computer's browser (if the Falcon is connected to a network).

When using Drive to File mode (DD, E01, or EX01), log files are also stored in the Destination drive in the same folder as the image files.

The log files in the Destination drive are available in PDF, HTML, and XML formats.

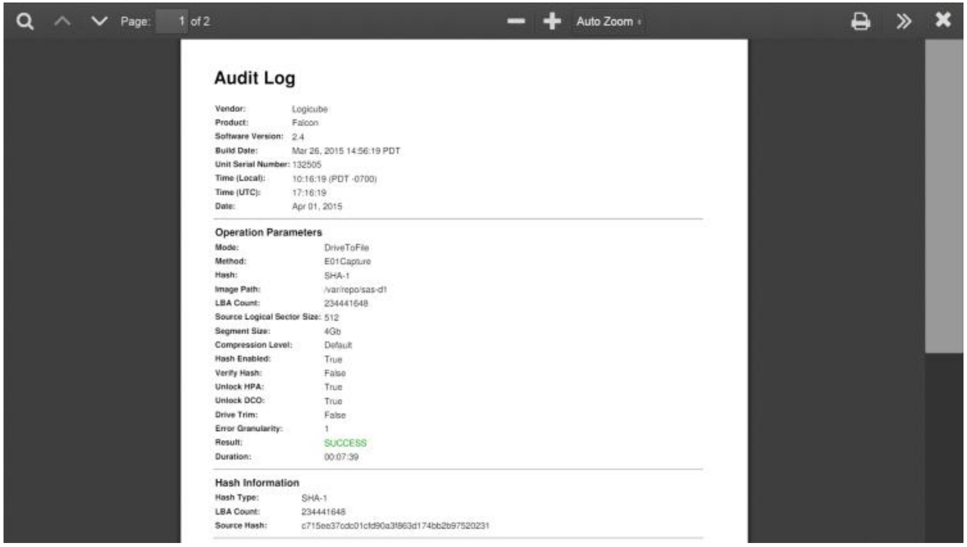
In addition to viewing, the logs can be exported to an external USB location such as a USB flash drive. Logs are exported in PDF, HTML and XML format.

From this screen, log files can also be deleted one at a time or all at once.



LOG FILE NAME	DATE CREATED
WIPE-74	TUE NOV 12 15:08:47 2013
WIPE-73	TUE NOV 12 14:39:23 2013
WIPE-72	TUE NOV 12 14:34:12 2013
	TUE NOV 12 13:18:44

Sample log viewed on-screen:



Audit Log

```
Vendor:                     Logicube
Product:                    Falcon
Software Version:           2.4
Build Date:                 Mar 26, 2015 14:56:19 PDT
Unit Serial Number:         132505
Time (Local):               10:16:19 (PDT -0700)
Time (UTC):                 17:16:19
Date:                       Apr 01, 2015

Operation Parameters
Mode:                       DriveToFile
Method:                     E01Capture
Hash:                       SHA-1
Image Path:                 /var/repo/sas-d1
LBA Count:                  234441648
Source Logical Sector Size: 512
Segment Size:               4Gb
Compression Level:          Default
Hash Enabled:               True
Verify Hash:                False
Unlock HPA:                 True
Unlock DCO:                 True
Drive Trim:                 False
Error Granularity:          1
Result:                     SUCCESS
Duration:                   00:07:39

Hash Information
Hash Type:                  SHA-1
LBA Count:                  234441648
Source Hash:                c715ee37cdc01cfd90a3f863d174bb2b97520231
```

The log file may contain several sections, depending on what settings and options were chosen during the operation, including:

- Information on the Falcon and its settings
- Case info (if entered)
- Source and Destination hashes

See **Section 3.8.1** for instructions on how to export the log files. See **Section 3.8.2** for instructions on how to delete the log files. See **Section 3.8.3** for instructions on how to Accessing the logs over a network.

6.0.9 Statistics

This will display two tabs: ***About*** and ***Adv. Drive Statistics***. The ***About*** screen will show information about the Forensic Falcon including the current software installed. Some of the information available in the ***About*** tab are:

- **Date –** The current date.
- **LocalTime –** The current local time
- **UTCTime –** The current UTC time
- **Version –** The current software version
- **BuildDate –** The build date of the software
- **KernelVersion –** The current kernel version
- **HostName –** The hostname that can be used when connecting to the Falcon via a network
- **N/W Interfaces –** Shows Ethernet adapter information such as the IP address, MAC address, and link speed
- **SerialNumber –** The serial number of the Falcon unit
- **SCSI Option –** Shows whether the SCSI module is attached or not
- **Uptime –** The total time the Falcon has been running since it was last turned on
- **BIOS Build Date –** Shows the BIOS build date

The ***Adv. Drive Statistics*** tab shows S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) information taken directly from what the drive is reporting. Navigate between drives by using the left and right scroll arrows. The up and down scroll arrows scroll through the different information. The information shown is the raw value tracked by the drive and is not translated.

6.0.10 Manage Repositories

Repositories can be added to the Falcon in this operation. Repositories can act as a Source or Destination.

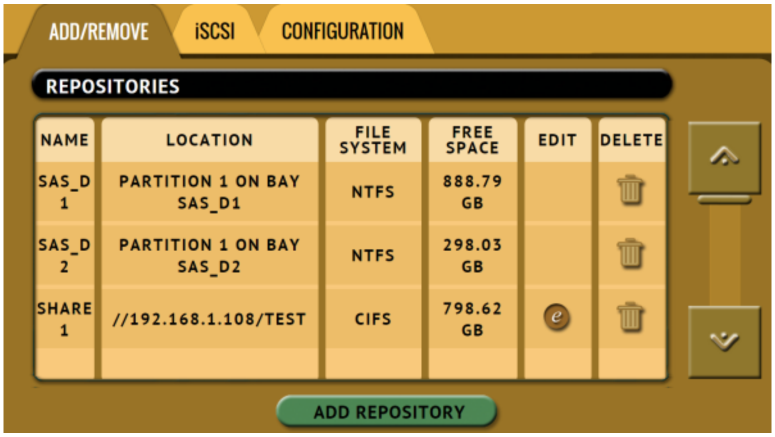
When ***Manage Repositories*** is selected, two tabs are available at the top of the screen:

- Add/Remove (using the SMB (Server Message Block) and CIFS (Common Internet File System) protocols)
- iSCSI (Internet Small Computer System Interface protocol)

Networks are configured differently and may require the assistance of a Network or Systems Administrator.

6.0.10.1 Add/Remove

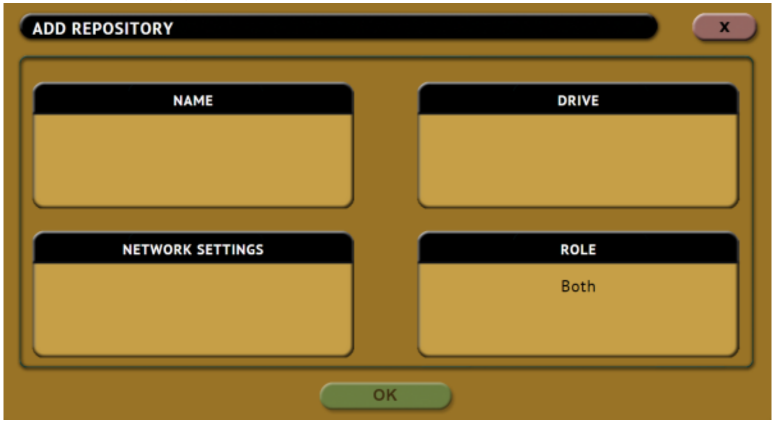
A list of repositories will be shown including local Destination drives and networked repositories. The user has the option of adding or deleting a repository.



REPOSITORIES

NAME	LOCATION	FILE SYSTEM	FREE SPACE	EDIT	DELETE
SAS_D 1	PARTITION 1 ON BAY SAS_D1	NTFS	888.79 GB		🗑
SAS_D 2	PARTITION 1 ON BAY SAS_D2	NTFS	298.03 GB		🗑
SHARE 1	//192.168.1.108/TEST	CIFS	798.62 GB	e	🗑

Tap ***Add Repository*** to add a repository. The Add Repository window will appear.



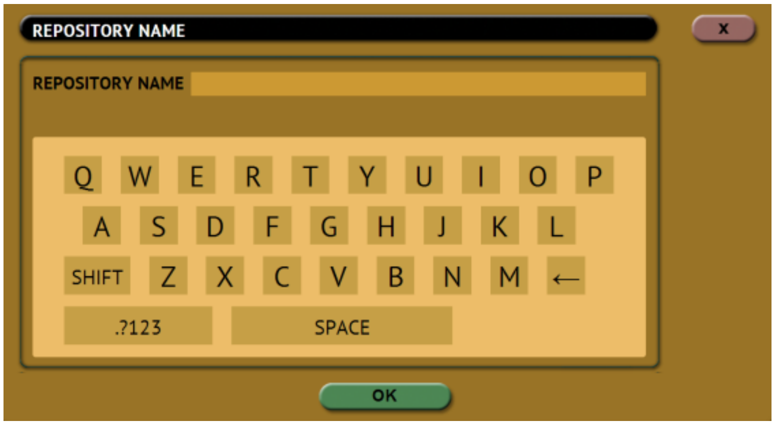
NAME

DRIVE

NETWORK SETTINGS

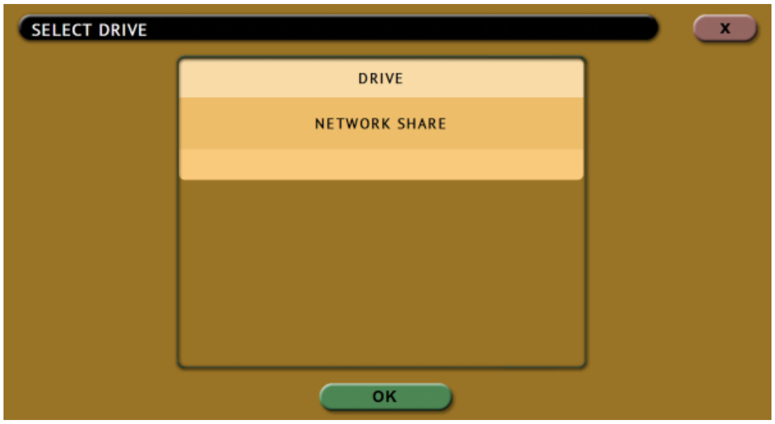
ROLE
Both

Tap ***Name*** to set the name of the repository. Tap the ***OK*** icon when finished.

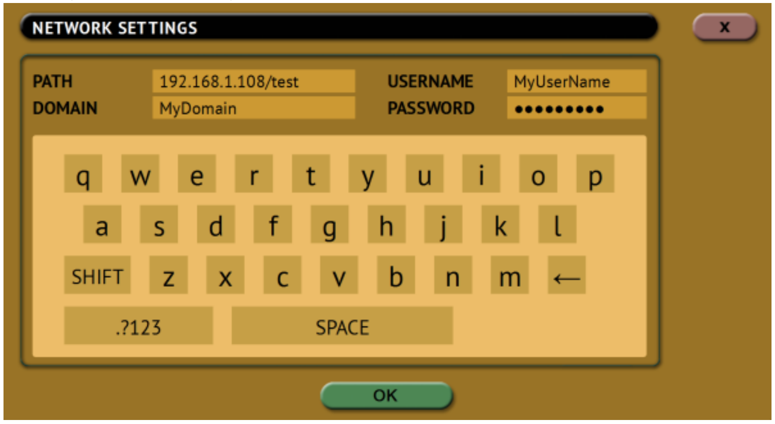


REPOSITORY NAME

Tap ***Drive*** to select a drive or network share to set as a repository. Tap the ***OK*** icon when finished.



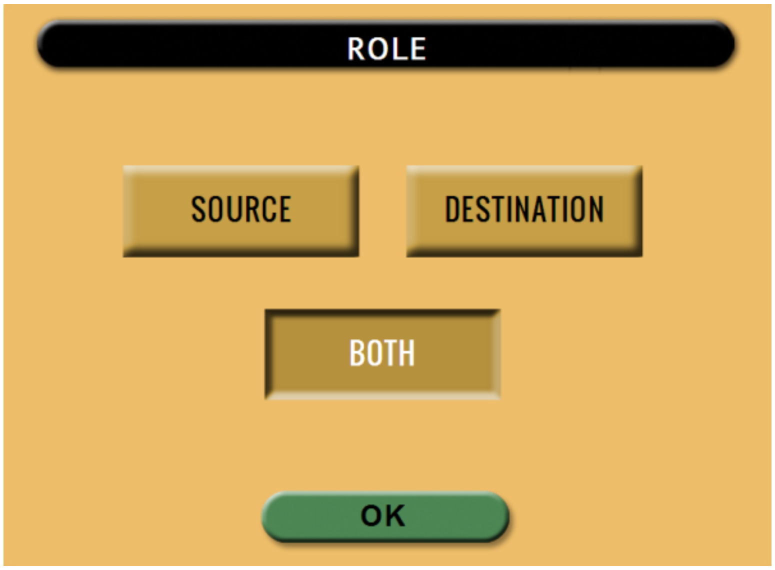
Tap ***Network Settings*** to enter the network settings. See the example below. Tap the ***OK*** icon when finished.


PATH 192.168.1.108/test
DOMAIN MyDomain
USERNAME MyUserName
PASSWORD ●●●●●●●●●

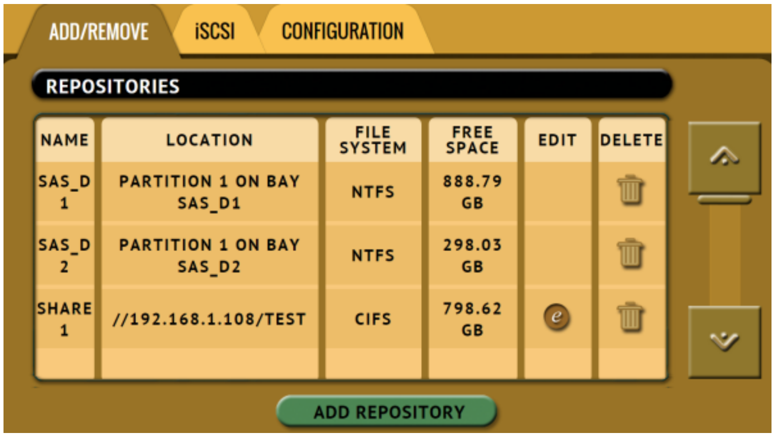
For the path, enter the IP address or hostname followed by a slash (/) then the share name. For example:
ip_or_hostname/sharename

Hidden Samba network shares (shares ending with $ can be mounted by adding the $ at the end of the share name. For example:
ip_or_hostname/sharename$

Tap ***Role*** and input the role for this repository. Tap ***OK*** when finished.



The repository will only appear as a Source when ***File to File*** imaging **is chosen.**



NAME	LOCATION	FILE SYSTEM	FREE SPACE	EDIT	DELETE
SAS_D 1	PARTITION 1 ON BAY SAS_D1	NTFS	888.79 GB		🗑
SAS_D 2	PARTITION 1 ON BAY SAS_D2	NTFS	298.03 GB		🗑
SHARE 1	//192.168.1.108/TEST	CIFS	798.62 GB	ⓔ	🗑

To edit a repository, tap the ⓔ ***(edit)*** icon. This will allow changes to the ***path, domain, username, or password***.

To delete a repository, tap the 🗑 ***(delete)*** icon. A confirmation screen will appear. Tap ***Yes*** to permanently delete the repository from the list.

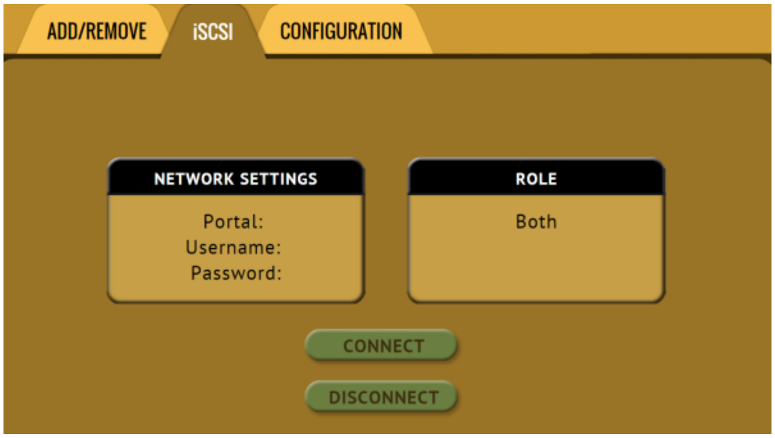
In order for a repository to remain configured when the Falcon is turned off, the changes must be saved and loaded to a configuration file. Details on configuration files can be found in ***Section 6.0.11.1***.

6.0.10.2 iSCSI

This screen allows a user to add a repository using the iSCSI protocol.

To add a repository using the iSCSI protocol, an iSCSI Target must be setup on the remote system. Since networks are configured differently, a Systems Administrator or Network Administrator may be needed to set up the iSCSI protocol.

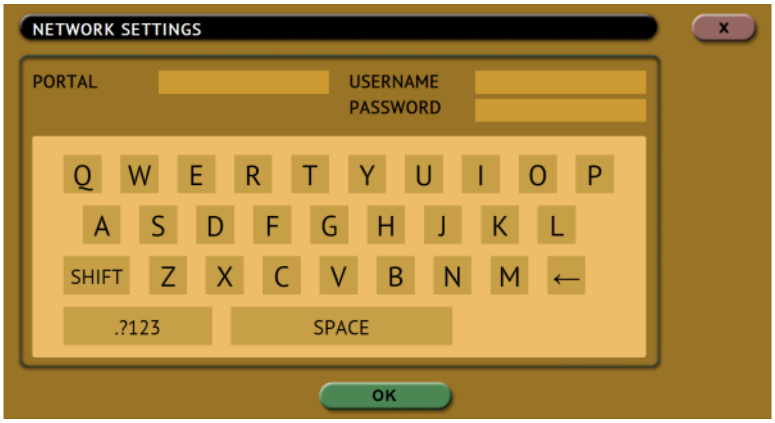
Once the iSCSI Target has been setup, tap ***Settings***.



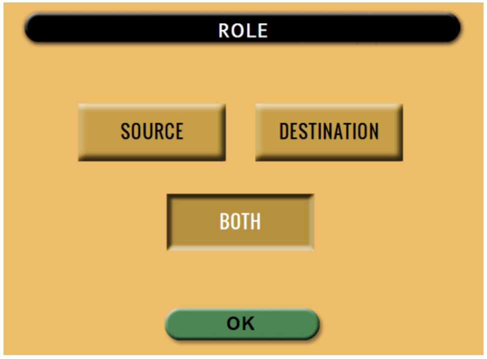
Portal:
Username:
Password:

ROLE
Both

Input the iSCSI target portal, username and password. Tap the ***OK*** icon when finished.



Tap ***Role*** and input the role for the iSCSI server then tap ***OK***.



6.0.11 System Settings

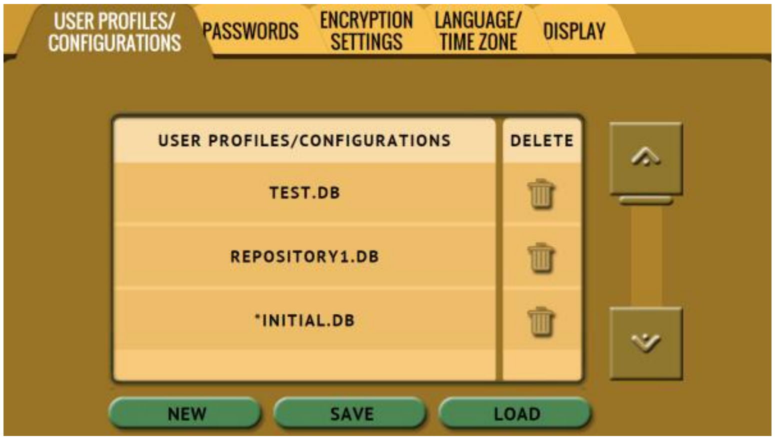
The ***System Settings*** screen allows users to configure five different settings for the Falcon:

- User Profiles/Configurations
- Passwords
- Encryption Settings
- Language/Time Zone
- Display

6.0.11.1 User Profiles/Configurations

This screen shows all user profiles/configurations for the Falcon. There are three options in this screen:

- **New –** Allows the user to create a new profile/configuration name.
- **Save –** Saves the selected profile/configuration.
- **Load –** Loads the selected profile/configuration.



USER PROFILES/CONFIGURATIONS	DELETE
TEST.DB	🗑
REPOSITORY1.DB	🗑
*INITIAL.DB	🗑

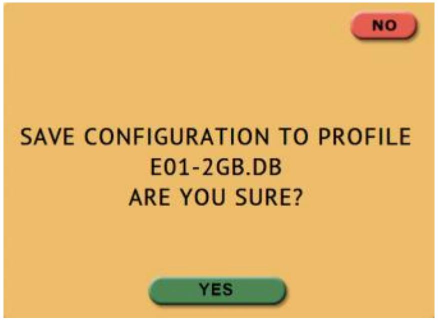
The Falcon will boot with the profile/configuration that has an asterisk (*) next to the name.

User Profiles/Configurations can be copied from one Falcon to another using the Command Line Interface. Profiles/Configurations can also be backed up to a USB flash drive and restored if needed. More information including detailed step-by-step instructions can be found in ***Section 10.6.***

Profiles/configurations allow users to create different profiles or configurations. The profile/configuration can then be saved. When a profile/configuration is loaded using the ***Load*** icon, the Falcon will load that configuration during its boot process.

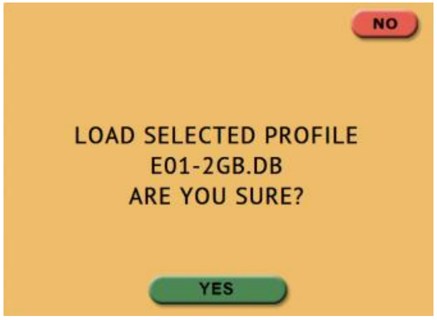
For example, if the user wants the Falcon to always boot up with the default imaging mode to ***Drive to File*** with the setting of ***E01*** with a segment size of ***2GB***:

1. Turn the Falcon off then back on. This will reset all settings to its default configuration. This is an important step to help ensure only the changes desired will be the changes saved.
2. Go to the ***Imaging*** screen and set the ***Mode*** to 'Drive to File.
3. In the ***Settings***, set the image to ***E01*** and set the segment size to ***2GB***.
4. In the ***System Settings***, go to ***User Profiles/Configurations*** and tap the ***New*** icon.
5. Type a name for this profile. For example, E01-2GB and tap the ***OK*** icon. The profile name should appear on the screen.
6. Tap the newly saved profile and tap ***Save***. A confirmation screen will appear:



SAVE CONFIGURATION TO PROFILE
E01-2GB.DB
ARE YOU SURE?

7. Tap the ***Yes*** icon to save the profile.
8. Make sure the profile to be loaded (during the boot process) is highlighted (in this case, E01-2GB.DB) and tap the ***Load*** icon. A confirmation screen will appear:



LOAD SELECTED PROFILE
E01-2GB.DB
ARE YOU SURE?

9. The next time the Falcon is turned on it will load the E01-2GB.DB profile.

To delete a profile, tap the 🗑 (delete) icon. A confirmation screen will appear. Tap the ***Yes*** icon to delete the selected profile.

It is highly recommended that the Falcon is turned off then back on before making any changes to the profiles/configurations. This helps ensure that only the desired changes are saved.

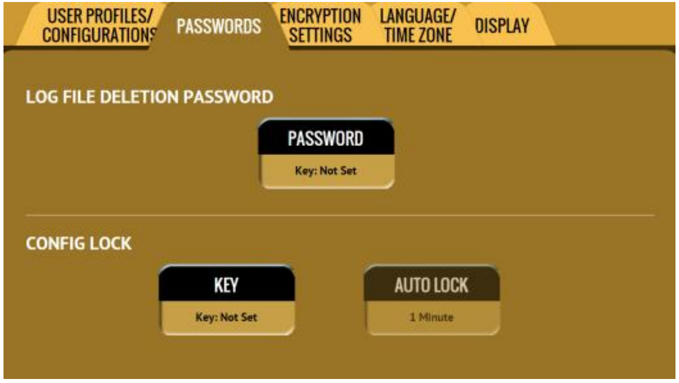
Do not highlight and save over the INITIAL.DB configuration. This is the default configuration of the Falcon and is used to reset the Falcon to the factory default settings.

6.0.11.2 Passwords

There are two sets of passwords that can be entered on the Falcon.

- **Log File Deletion Password –** A password can be set as an extra layer of protection when deleting log files. If this password is set, Falcon will prompt for the password before any log files can be deleted.
- **Config Lock –** The Falcon can be configured to lock out any configuration changes. When this is enabled, changes to the different types of operations cannot be made without entering the correct key or password. Different types of operations can still be started.

  For example, when the Falcon is locked, and it is configured for Drive to Image Imaging mode, the user will be unable to change this mode to Drive to Drive or File to File, but can start the Drive to Image task.



LOG FILE DELETION PASSWORD

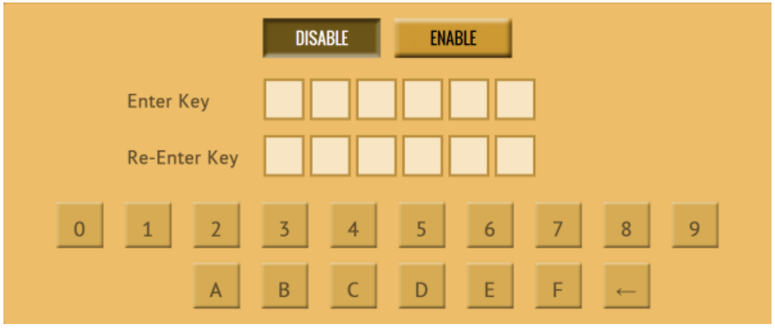
PASSWORD
Key: Not Set

CONFIG LOCK

KEY
Key: Not Set

AUTO LOCK
1 Minute

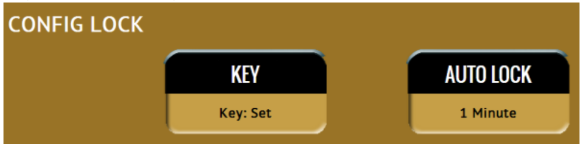
Tap ***Password*** or ***Key*** to enter a log file deletion password or a config lock key. The following screen will appear.



Tap the ***Enable*** icon to enter a password or key. The available characters are 0 through 9 and A through F.

6.0.11.2.1 Additional information for Config Lock

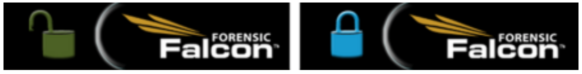
Tap the ***Auto Lock*** icon to set the time to automatically lock the configuration and require a password. By default, this is set to 1 minute.



KEY
Key: Set

AUTO LOCK
1 Minute

A shortcut (and indicator) to the ***config lock*** can always be seen on the Falcon's screen. It is located on the top-right of the screen, next to the Falcon logo.



While in a locked state, the following operations will be affected as follows:

- **Imaging –** An imaging task can be started, but no settings can be changed. Additionally, no new task can be added, and no task can be deleted without the unlock key.
- **Hash –** A hash task can be started, but no settings can be changed. Additionally, no new task can be added, and no task can be deleted without the unlock key.
- **Wipe –** A wipe task can be started, but no settings can be changed. Additionally, no new task can be added,

and no task can be deleted without the unlock key.

- **Task Macro –** A task macro can be started, but no settings can be changed. Additionally, no new macro can be set or edited without the unlock key.
- **USB Device –** Since there are no settings or configurations for this operation, it is not affected by Config Lock.
- **File Browser –** The file browser cannot be accessed without the unlock key.
- **Logs –** Since there are no settings or configurations for this operation, it is not affected by Config Lock.
- **Statistics –** Since there are no settings or configurations for this operation, it is not affected by Config Lock.
- **Manage Repositories –** A managed repository cannot be added without the unlock key. At this time, a managed repository can be deleted without the unlock key. A future software update will require the unlock key to delete a managed repository.
- **System Settings –** This entire section cannot be accessed without the unlock key.
- **IP Settings –** This entire section cannot be accessed without the unlock key.
- **Software Updates –** This entire section cannot be accessed without the unlock key.
- **Power Off –** This entire section cannot be accessed without the unlock key.

The Passwords can be saved into a user profile/configuration and loaded each time the Falcon is turned on. See **Section 6.0.10.1** for more information on saving and loading a user profile/configuration.

The Falcon can still be turned off without the unlock key by using the power switch located in the back of the Falcon.

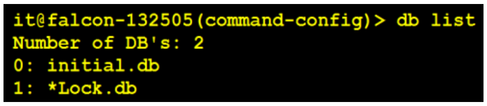
Remember the Config Lock Key! If the Falcon is configured to load with the Config Lock set (enabled) the only way to delete the Config Lock is to reset the Falcon using the Command Line Interface (CLI).

6.0.11.2.2 Forgotten password or config lock key

If the Log File Deletion password or Config Lock key is forgotten, the Falcon will need to be reset using the Command Line Interface (CLI). See **Section 10.2** for more information on how to connect to the Falcon using the CLI.

Once connected to the CLI:

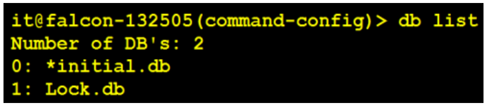
1. Login with the username “***it***” (without the quotes) and the password “***it***” (without the quotes).
2. From the main prompt, type ***command*** then press the enter key.
3. Type ***config*** then press the enter key.
4. Type ***db list*** then press the enter key. This will show a list of databases or configurations saved. The example below shows two databases (the default initial.db and Lock.db). The db that shows an asterisk (*) before the name is the current database or configuration being loaded each time the Falcon is turned on.



```
it@falcon-132505(command-config)> db list
Number of DB's: 2
0: initial.db
1: *Lock.db
```

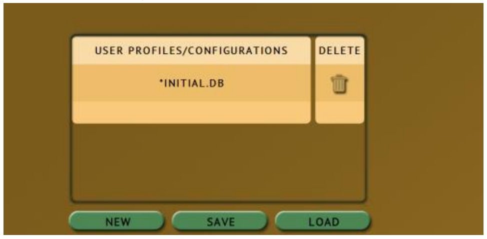
5. Type ***db load initial.db*** then press the Enter key to load the default database. There should be a response showing “Command (DbManagement) Successful”.

6. Type ***db list*** again and there should be an asterisk (*) on initial.db.



```
it@falcon-132505(command-config)> db list
Number of DB's: 2
0: *initial.db
1: Lock.db
```

7. Turn the Falcon off using the power switch located in the back of the device, and close the Telnet/SSH application.
8. Wait for the Falcon to completely turn off then turn it back on. When the Falcon boots up, it will load the default configuration. The default configuration can be checked by going to ***System Settings*** and looking at the ***User Profiles/Configurations*** tab. INITIAL.DB should have an asterisk next to it (as seen below).



6.0.11.3 Encryption Settings

The Falcon allows imaging drives onto a Destination where the data on the Destination drive is encrypted. Destination drives that are encrypted by the Falcon can be decrypted by using the Falcon or third party software (TrueCrypt or FreeOTFE).

For in-depth information on encrypting and decrypting a drive using the Falcon, or decrypting a drive using TrueCrypt or FreeOTFE, please see **Chapter 8: Drive Encryption and Decryption.**

There are 4 parameters that must be configured before encryption can be used. These 4 parameters are necessary to decrypt and read the Destination drive properly:

- **Cipher Mode** – Users can choose between ***TC-XTS***, ***CBC*** (cbc-plain64.) or ***ECB*** (cbc-essiv:sha256) cipher modes.
- **Cipher** – At this time, only the ***AES-256*** cipher is supported.

- **IV Generation** – Unavailable when TC-XTS cipher mode is selected. If CBC or ECB cipher mode is selected, users can choose between ***PLAIN64*** and ***ESSIV:SHA256***.
- **Encryption** (Password or Key) – Users must choose their own encryption password/key.

There are 2 imaging modes in which encryption can be used:

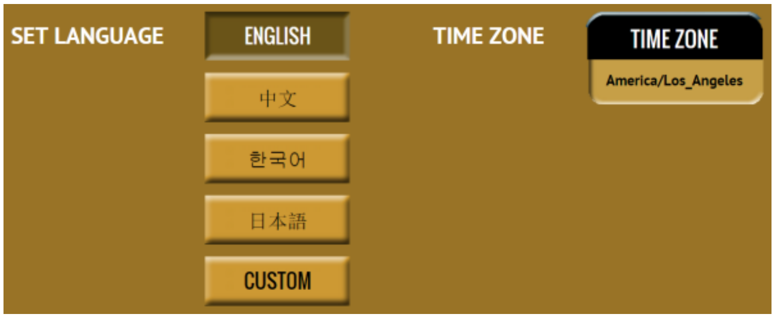
- **Drive to File** – Images the Source to any of the following image output formats: ***DD***, ***E01***, and ***EX01***. This will have a partition level encryption where only the partition (on the Destination or Repository) where the images are created will be encrypted.
- **File to File** – Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source and each file will be hashed. This will have a partition level encryption where only the partition (on the Destination or Repository) where the images are created will be encrypted.

There are many articles on the Internet about AES-256 encryption and the different modes and settings that come with encryption.

6.0.11.4 Language/Time Zone

The Falcon's menu system's language can be changed. At this time, the available languages are English, Chinese (中文), Korean (한국어), and Japanese (日本語).

This screen also allows the time zone to be set.



6.0.11.4.1 Language

Four languages are available at this time. Select English, Chinese (中文), Korean (한국어), or

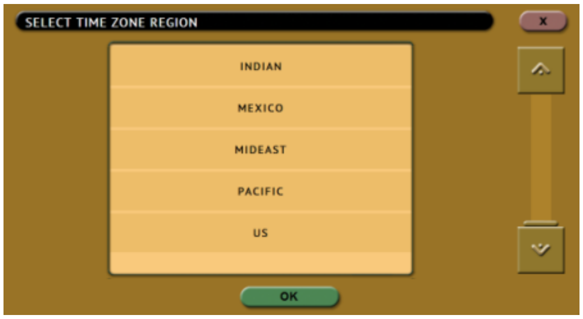
Japanese (日本語) to change the language displayed. As soon as the selection is made, the Falcon's screen (or the computer's Internet browser) will automatically refresh and display the selected language.

The ***Custom*** button is reserved for future language releases.

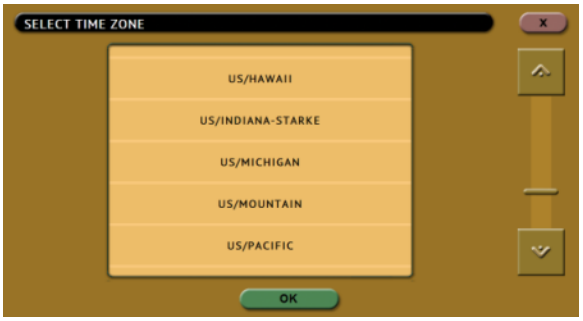
6.0.11.4.2 Time Zone

The Falcon utilizes NTP (Network Time Protocol). Each time the Falcon is connected to a network with internet access, it will automatically check for the correct time using NTP and adjust the time as needed.

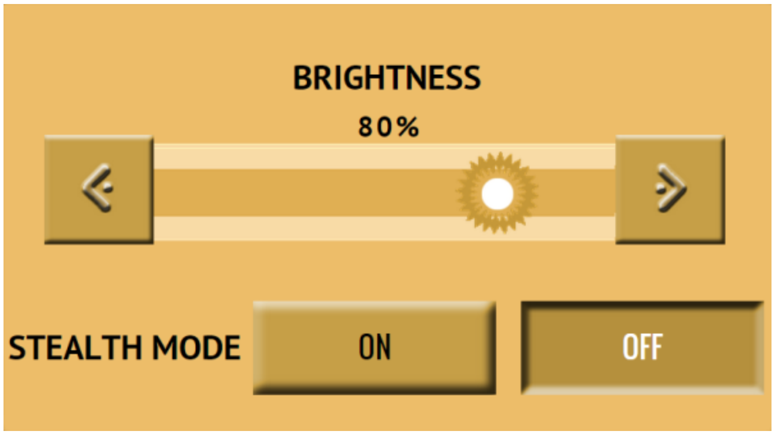
The Falcon also has a time zone setting. Tap ***Time Zone*** to select the time zone region. Tap the ***OK*** icon to continue.


SELECT TIME ZONE REGION

After selecting the region, select the time zone where the Falcon is located. Tap the ***OK*** icon to set the time zone.


SELECT TIME ZONE

6.0.11.5 Display



Brightness – The Falcon's screen's brightness may need to be adjusted, depending on the user's preference. To adjust the brightness, use the left or right arrow icons on the screen. The screen's brightness will adjust accordingly.

The screen brightness cannot be saved and loaded as a user profile/configuration. Each time the Falcon boots, the brightness will be reset to 80%.

Stealth Mode – Stealth mode turns the Falcon's screen off, allowing privacy so no one can see what the Falcon is doing. When Stealth mode is activated, currently running operations continue to run.

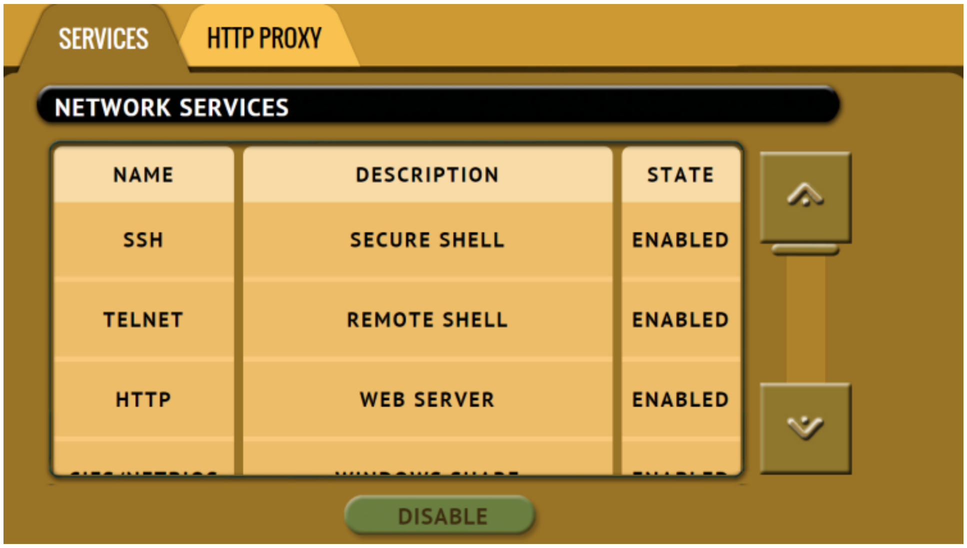
To turn Stealth mode on, tap ***ON***.

To turn Stealth mode off and restore the Falcon's display, tap anywhere on the screen.

Stealth mode will not have any effect on the computer's Internet browser.

6.0.12 Network Settings

The Network settings screen allows certain services to be enabled or disabled in the ***Services*** tab. There is also an ***HTTP Proxy*** tab where proxy server information can be entered.



NAME	DESCRIPTION	STATE
SSH	SECURE SHELL	ENABLED
TELNET	REMOTE SHELL	ENABLED
HTTP	WEB SERVER	ENABLED

6.0.12.1 Services

There are 7 services that can be disabled (enabled by default):

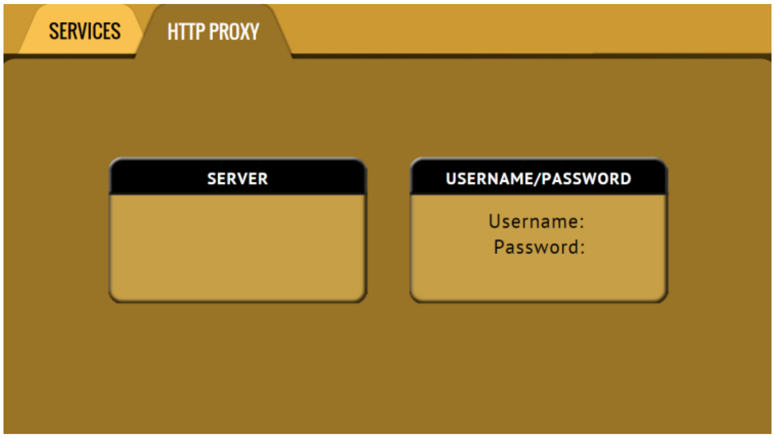
- **SSH –** Disabling this will block Secure Shell (SSH) traffic.
- **Telnet –** Disabling this will block Telnet traffic.
- **HTTP –** Disabling this will block web browser connections to the Falcon.
- **CIFS/NETBIOS –** Disabling this will block any CIFS or NETBIOS connection to the Falcon (for example, Windows Explorer).
- **iSCSI –** Disabling this will block iSCSI connections.
- **Iperf –** Disabling this will block Iperf traffic (a network tool to measure bandwidth performance).
- **Ping –** Disabling this will block ping access to the Falcon.

Disabling any of the services above will disallow the types of communication controlled by those services. For example, if HTTP is disabled, users will not be able to see the Falcon through a web browser over the network.

Please contact your Network or Systems Administrator before changing any of these services.

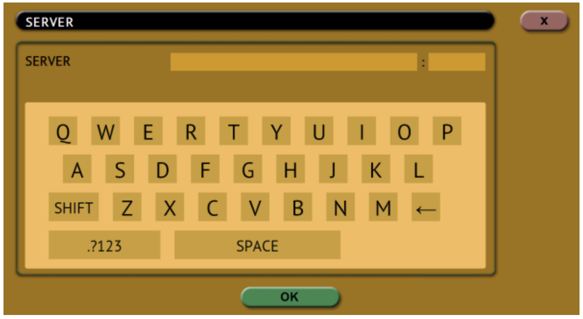
6.0.12.2 HTTP Proxy

If the network the Falcon is connected to uses an HTTP proxy server to access the Internet, a proxy settings may need to be set in order for the Falcon to be able to update software from a network (over the internet),. This typically includes a server (or IP address), a host port, a username and password.



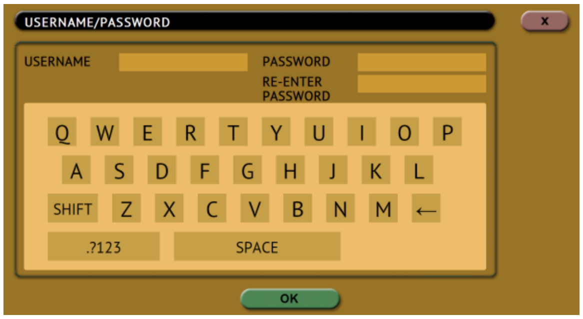
6.0.12.2.1 Server

Tap the Server icon to set the IP address (or server name) and port of the proxy server.



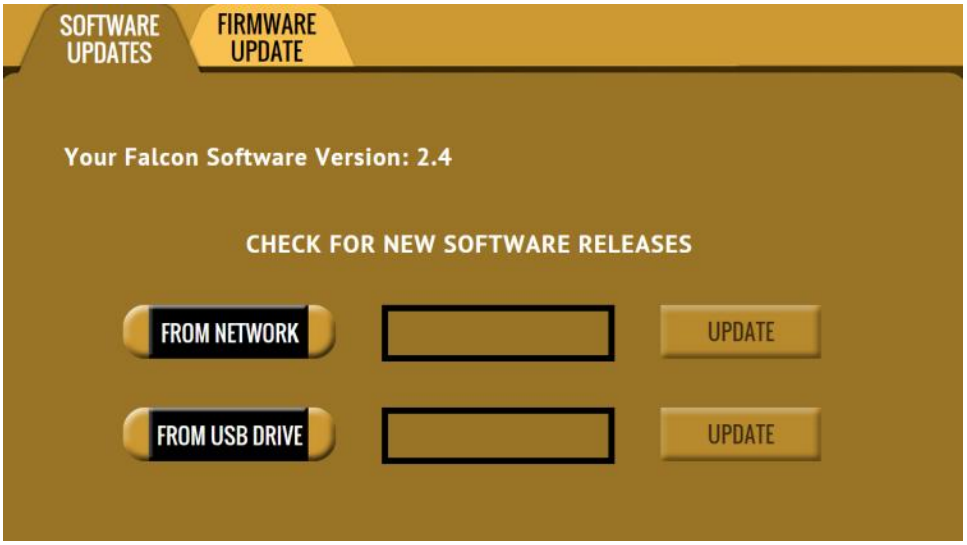
6.0.12.2.2 Username/Password

If the proxy server requires a username and password for authentication, tap the ***Username/Password*** icon to set this information.



6.0.13 Software Update

New and improved software will be released from time to time. There are two ways to update the software on the Falcon: From the web via a network connection or from a USB drive.



Your Falcon Software Version: 2.4

For the latest step-by-step instructions on how to update the Falcon software, please read the ***Falcon Software readme*** file located on the following site: http://www.logicube.com/knowledge/forensic-falcon

In-depth information on updating the Falcon software can be found in **Chapter 9: Updating the Falcon Software**.

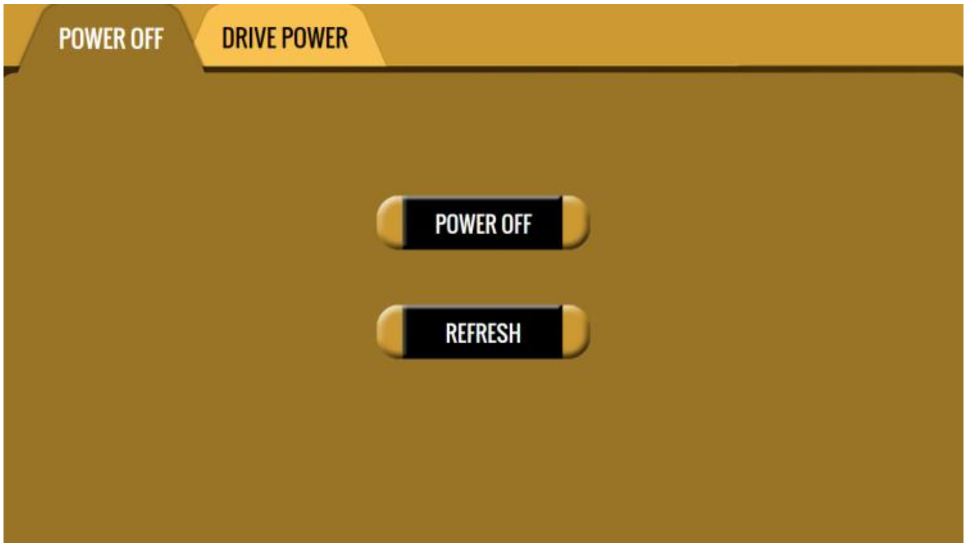
6.0.14 Power Off

There are two tabs in the ***Power Off*** screen:

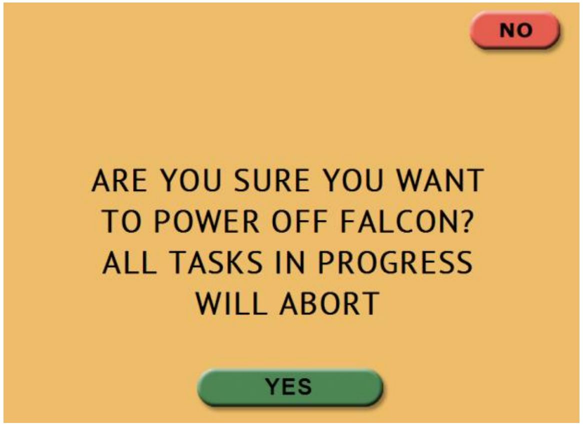
POWER OFF – The Falcon can be remotely turned off by going to this tab. Additionally, the Graphical User Interface (GUI) can be refreshed.

DRIVE POWER – Inactive drives connected to the Falcon can be set to go to standby mode in this tab. The default is set to 0 minutes (OFF).

Power Off screen:

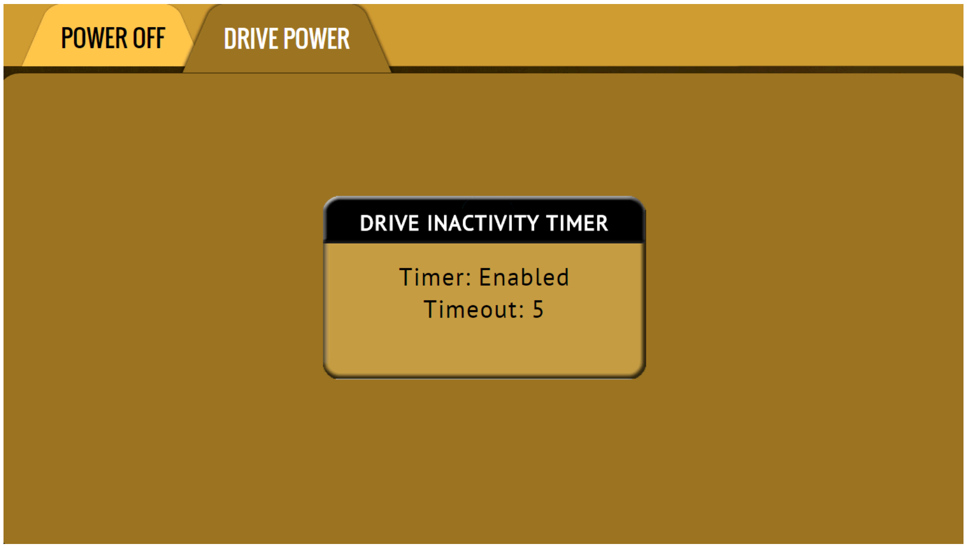


A confirmation screen will appear. Select ***Yes*** to confirm the selection.



ARE YOU SURE YOU WANT TO POWER OFF FALCON? ALL TASKS IN PROGRESS WILL ABORT

Drive Power screen:



DRIVE INACTIVITY TIMER

Timer: Enabled
Timeout: 5

7: Viewing EXT4 formatted Destination drives in Windows

7.0 Introduction

The Falcon formats Destination drives using the NT File System (NTFS) or EXT4 file system. Linux Operating Systems have native support for EXT4 file systems. Windows, however, does not have native support for viewing the EXT4 file system. There are several utilities that allow viewing of the EXT4 file system in Windows. ***Ext2Fsd*** (http://www.ext2fsd.com/) is a free, open source utility driver allows EXT3 and EXT4 partitions to be viewable in Windows.

The Falcon labels the formatted Destination drive as "**REPOSITORY**".

Logicube does not provide full support for Ext2fsd. We provide basic instructions on how to make this utility work in our scenario. For Ext2fsd support, please visit their website above.

7.0.1 Step-by-step instructions – Using Ext2fsd

1. Download and install Ext2fsd from the website above. If Ext2fsd is already installed, skip to step 2.

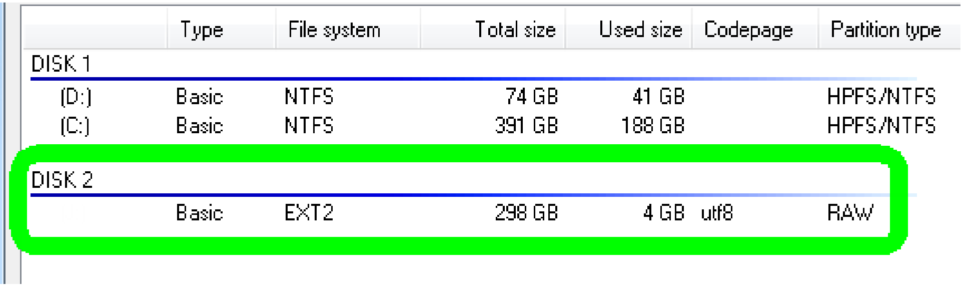
After installing Ext2fsd, reboot the computer.

2. Connect the Destination drive to the computer. The Falcon can be used to view the Destination drive. See ***Sections 3.6 and 6.0.6*** for more information. Alternatively, other methods can be used to connect the drive to the computer (e.g. a write block device).

There are times when Windows will auto-assign a drive letter to the drive. If it auto-assigns a drive letter at this point, continue with the analysis process. There is no need to follow the other steps in these instructions. If Windows does not auto-assign a drive letter, open Ext2fsd's ***Ext2 Volume Manager*** program.

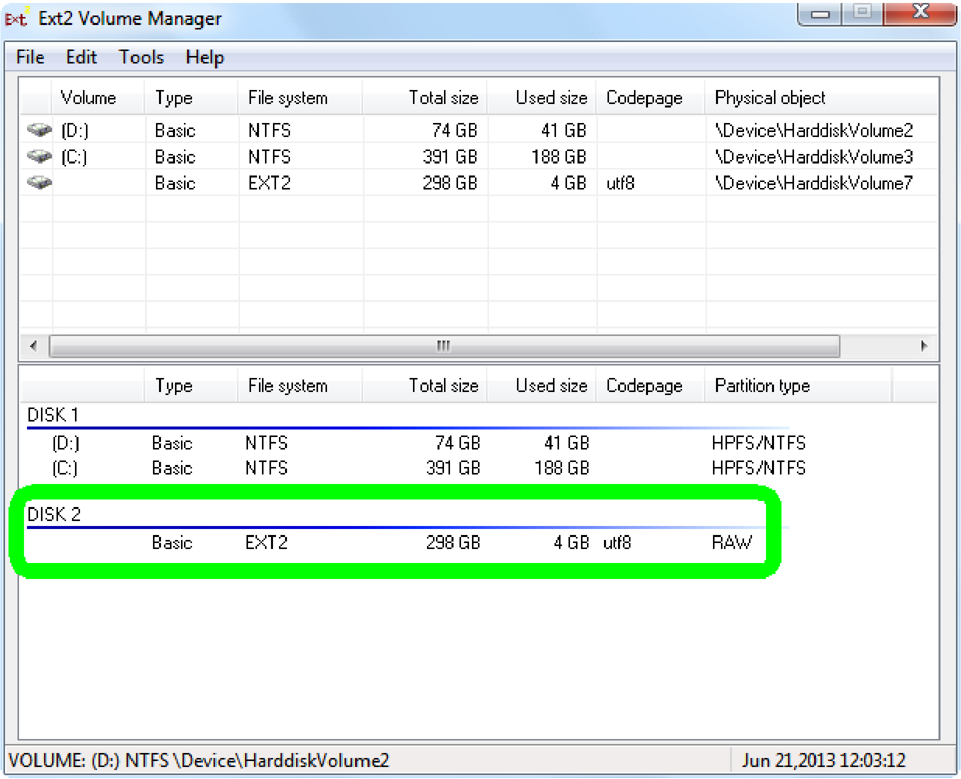
3. Locate the Destination drive. The Destination drive should have a ***RAW*** "Partition type".

NOTE: Here is a close-up screen shot of what the Destination drive will look like in the Ext2 Volume Manager program. Note the Partition type is set to RAW.



	Type	File system	Total size	Used size	Codepage	Partition type
DISK 1						
(D:)	Basic	NTFS	74 GB	41 GB		HPFS/NTFS
(C:)	Basic	NTFS	391 GB	188 GB		HPFS/NTFS
DISK 2						
	Basic	EXT2	298 GB	4 GB	utf8	RAW

Here is a screen shot of the full Volume Manager window.

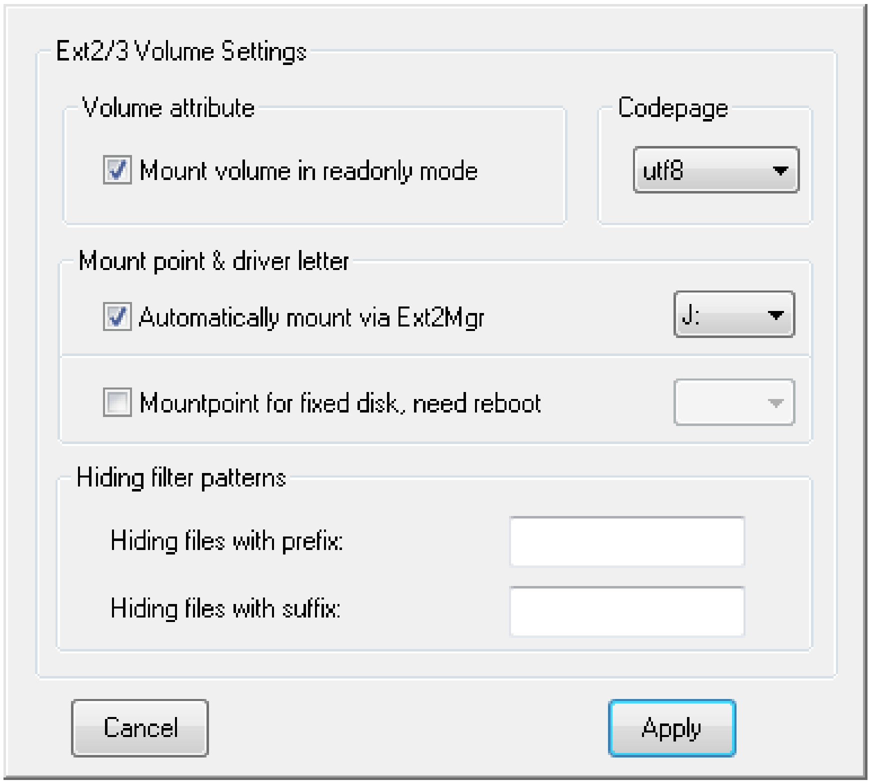


Volume	Type	File system	Total size	Used size	Codepage	Physical object
(D:)	Basic	NTFS	74 GB	41 GB		\Device\HarddiskVolume2
(C:)	Basic	NTFS	391 GB	188 GB		\Device\HarddiskVolume3
	Basic	EXT2	298 GB	4 GB	utf8	\Device\HarddiskVolume7

	Type	File system	Total size	Used size	Codepage	Partition type
DISK 1						
(D:)	Basic	NTFS	74 GB	41 GB		HPFS/NTFS
(C:)	Basic	NTFS	391 GB	188 GB		HPFS/NTFS
DISK 2						
	Basic	EXT2	298 GB	4 GB	utf8	RAW

VOLUME: (D:) NTFS \Device\HarddiskVolume2 Jun 21,2013 12:03:12

4. Double-click the drive. Alternatively, the drive can be highlighted, then from the menu system, go to ***Tools*** then ***Ext2 Volume Management***. The following screen will appear. Make sure that there is a check mark next to “Automatically mount via Ext2Mgr. Also, make sure there is a drive letter assigned (to the right of this option). If not, assign an available drive letter. Click the ***Apply*** button.



Ext2/3 Volume Settings

Volume attribute

☑ Mount volume in readonly mode

Codepage: utf8

Mount point & driver letter

☑ Automatically mount via Ext2Mgr J:

□ Mountpoint for fixed disk, need reboot

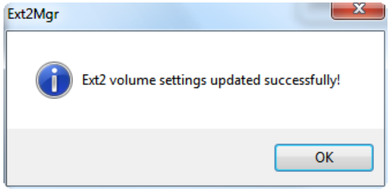
Hiding filter patterns

Hiding files with prefix:

Hiding files with suffix:

Do not uncheck the "Mount volume in readonly mode" unless it is absolutely certain that the mounted drive needs to be over-written or erased (whether partially or fully).

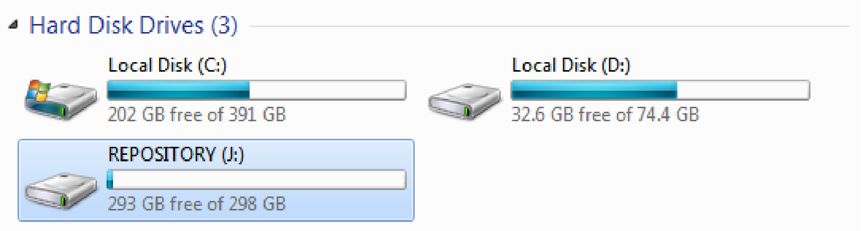
5. The following confirmation screen will appear. Click ***OK*** to continue.



Ext2Mgr

Ext2 volume settings updated successfully!

6. Close the Ext2fsd Volume Manager program. Windows should now see the drive and assign it a drive letter with the volume name "**REPOSITORY**".



Hard Disk Drives (3)

Local Disk (C:) 202 GB free of 391 GB

Local Disk (D:) 32.6 GB free of 74.4 GB

REPOSITORY (J:) 293 GB free of 298 GB

8: Drive Encryption and Decryption

8.0 Introduction

The Forensic Falcon allows imaging drives onto a Destination or Repository where the data on the Destination drive is encrypted. There are two different modes where Encryption is supported: Drive to File and File to File.

- **Drive to File –** Images the Source to any of the following image output formats: ***DD***, ***E01***, and ***EX01***. This will have a partition level encryption where only the partition (on the Destination or Repository) where the images are created will be encrypted.
- **File to File -** Image specific files (by filename, extension, etc.). The files will be sorted by path (based on where the file is located on the Source and each file will be hashed. This will have a partition level encryption where only the partition (on the Destination or Repository) where the images are created will be encrypted.

Falcon can also decrypt drives that were encrypted using the Falcon. Alternatively, third party utilities can be used to decrypt a drive encrypted by the Falcon; TrueCrypt and FreeOTFE.

In the ***System Settings*** screen, there is an ***Encryption Settings*** tab used to configure the Falcon for encryption. There are four (4) parameters that must be configured before encryption can be used. These parameters are necessary to decrypt and read the Destination drive and can be configured in the ***Encryption Settings*** page on the Falcon:

- **Cipher Mode –** Users can choose between ***TC-XTS***, ***CBC*** or ***ECB*** cipher modes.

> TC-XTS cipher mode can be decrypted using the Falcon or TrueCrypt.
>
> CBC or ECB cipher modes can be decrypted using the Falcon or FreeOTFE.

> The Falcon encrypts drives using AES 256 encryption regardless of what cipher mode is used. If TC-XTS is used, Falcon uses a TrueCrypt friendly format and **does not** use TrueCrypt to encrypt the drive. The encryption key is not stored on the Destination drive.

- **Cipher –** At this time, only the ***AES-256*** cipher is supported.
- **IV Generation –** Initialization Vector. Unavailable when TC-XTS cipher mode is selected. If CBC or ECB cipher mode is selected, users can choose between ***PLAIN64*** and ***ESSIV:SHA256***.
- **Encryption** (Password or Key) **–** Users must choose their own encryption password/key.

> There are many articles on the Internet about AES-256 encryption and the different modes and settings that come with encryption.

8.1 Encrypting a Destination

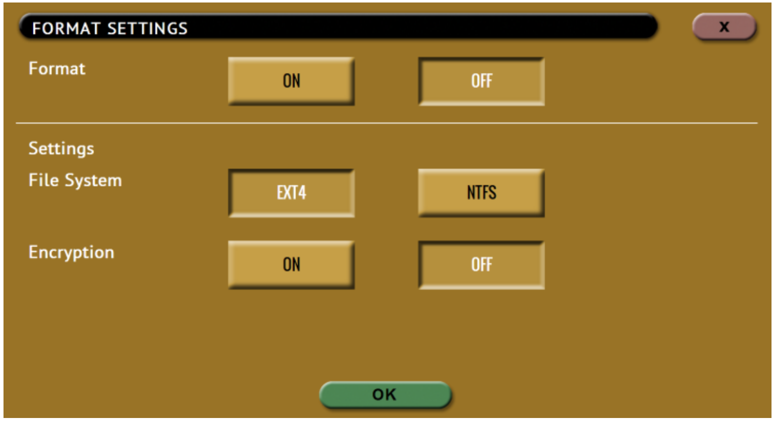
To encrypt a Destination, the Encryption settings must be set and the drive will need to be formatted using the Falcon. These steps must be performed prior to an Imaging operation.

8.1.1 Step-by-step Instructions

1. Select ***System Settings*** from the types of operation on the left side.
2. Tap the ***Encryption Settings*** tab.
3. Set the ***Cipher Mode***, ***Cipher***, ***IV Generation***, ***and Password***.
4. Select ***Wipe*** from the types of operation on the left side.
5. Tap the ***Destination*** icon and select the Destination drive to be formatted and encrypted.
6. Tap the ***Settings*** icon.

- If the Destination needs to be wiped, choose the type of wipe to be performed (Secure Erase and/or Wipe Patterns). If Wipe Patterns is selected, choose the type of Wipe Pattern to perform (DoD or Custom).
- If the drive has an HPA or DCO area that needs to be wiped, tap the ***HPA/DCO*** icon and select ***Yes*** to wipe the HPA or DCO area of the drive.
- If a Wipe Pattern was selected, tap the ***Passes*** icon to edit the number of passes and what gets written on each pass. If DoD was selected, a 7th pass value must be chosen.

7. Tap the ***Format Settings*** icon to change the Format setting.
   a. Set ***Format*** to ***ON***.
   b. Select the desired ***File System*** (***EXT4*** or ***NTFS***).
   c. Set ***Encryption*** to ***ON***. When finished, tap the ***OK*** icon.



FORMAT SETTINGS

Format: ON OFF

Settings

File System: EXT4 NTFS

Encryption: ON OFF

The Falcon will perform each of the settings sequentially. For example, if Secure Erase is set to ON, a Wipe Pattern mode is specified, and Format is set to On, the Falcon will first secure erase the drive, then wipe the drive according to the mode specified, then format the drive.

8. Tap the ***Start*** icon to start the wipe task. The Falcon will perform a Secure Erase first (if selected), then a Wipe Pattern (if selected), then finally a Format with encryption.

8.1.2 Using previously encrypted Destination drives

If a previously encrypted Destination drive is going to be used and the Falcon has been turned off since the last time the encrypted drive was used, the encryption settings must be set with the same encryption settings previously used before connecting the drive.

1. Turn the Falcon on. Make sure the previously encrypted Destination drive is not connected.
2. From the main menu, select ***System Settings*** from the types of operations on the left side.
3. Tap the ***Encryption Settings*** tab.
4. Set the ***Cipher Mode***, ***Cipher***, ***IV Generation***, and ***Password*** that was used for the previously encrypted Destination drive.
5. Connect the previously encrypted Destination drive to one of the Destination ports.

8.2 Decrypting a Falcon encrypted Destination drive with a Falcon

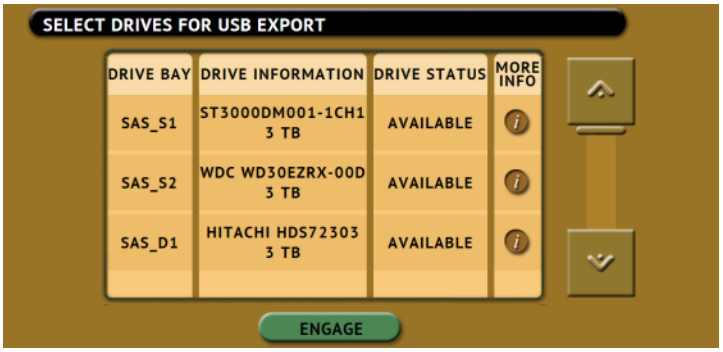
Falcon can decrypt a Destination drive encrypted by the Falcon. To decrypt the drive using a Falcon, the correct encryption settings must be set. After the encryption settings are set, the drive needs to be connected to the Falcon, and the Falcon can then be connected to a computer via USB.

If the Destination drive was formatted with the EXT4 file system, please read ***Chapter 7*** for information on how to view EXT4 in Windows.

8.2.1 Step-by-step Instructions

1. Turn the Falcon on. Make sure the previously encrypted Destination drive is **not** connected.

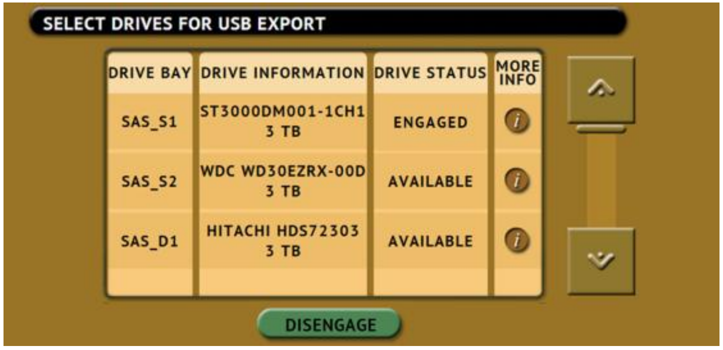
2. From the main menu, select ***System Settings*** from the types of operations on the left side.
3. Tap the ***Encryption Settings*** tab.
4. Set the ***Cipher Mode***, ***Cipher***, ***IV Generation***, ***and Password***. These should be set to the same values as to how the drive was encrypted. If the values are incorrect, the drive will not be decrypted properly and the data will be unrecognizable.
5. Connect the previously encrypted Destination drive to one of the Destination ports
6. Select ***USB Device*** from the types of operation on the left side. When this type of operating is selected, the following screen will appear:



SELECT DRIVES FOR USB EXPORT

DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_S1	ST3000DM001-1CH1 3 TB	AVAILABLE	ⓘ
SAS_S2	WDC WD30EZRX-00D 3 TB	AVAILABLE	ⓘ
SAS_D1	HITACHI HDS72303 3 TB	AVAILABLE	ⓘ

7. Choose the drive to be viewed then tap the ***ENGAGE*** icon. The 'DRIVE STATUS' for the selected drive will change to "ENGAGED" and the ***ENGAGE*** icon will change to ***DISENGAGE***. At this point, connect a USB cable between the computer and the Falcon.

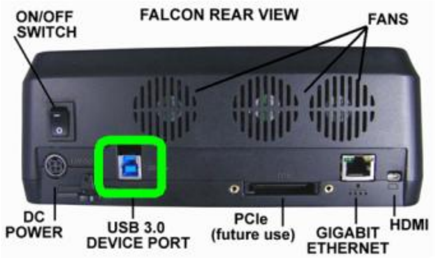


SELECT DRIVES FOR USB EXPORT

DRIVE BAY	DRIVE INFORMATION	DRIVE STATUS	MORE INFO
SAS_S1	ST3000DM001-1CH1 3 TB	ENGAGED	ⓘ
SAS_S2	WDC WD30EZRX-00D 3 TB	AVAILABLE	ⓘ
SAS_D1	HITACHI HDS72303 3 TB	AVAILABLE	ⓘ

8. Connect a USB cable (A to B USB cable, one was included with the Falcon) between the computer and the Falcon. Connect the USB B connector to the Falcon's USB Device Port located on the back panel of the Falcon. Connect the USB A connector to an available USB port on the computer.

When using this type of operation, use the **USB Device port** located on the back panel of the Falcon.



9. After a few moments, Windows should assign a drive letter to the selected drive. The contents of the drive should now be accessible in Windows.
10. When finished, tap the ***DISENGAGE*** icon to disengage the USB mode. The USB cable can now be disconnected from the computer and the Falcon.

If the data on the drive is unrecognizable, disconnect the drive, then double-check the encryption settings (steps 2 through 4), then re-connect the drive

8.3 Decrypting the drive without a Falcon

In order to mount and read an encrypted Destination drive in Windows, without using a Forensic Falcon, Logicube recommends one of two third-party utilities called ***TrueCrypt*** or ***FreeOTFE***. Other utilities may work, but are not supported or tested by Logicube.

TrueCrypt can be downloaded from (for decryption purposes only):
http://truecrypt.sourceforge.net/

FreeOTFE can be downloaded from:
http://sourceforge.net/projects/freeotfe.mirror/files/latest/download

To install FreeOTFE the verification of signed drivers must be disabled. Here is a link that might help:
http://en.kioskea.net/faq/3914-windows-7-disable-signature-verification-of-drivers

There are other ways of installing unsigned drivers. Several different ways can be found by searching the Internet for “install unsigned drivers”.

If the Destination drive was formatted with the EXT4 file system, please read ***Chapter 7*** for information on how to view EXT4 in Windows.

8.3.1 Which decryption software to use?

The decryption software to use (TrueCrypt or FreeOTFE) depends on how the Destination drive was encrypted.

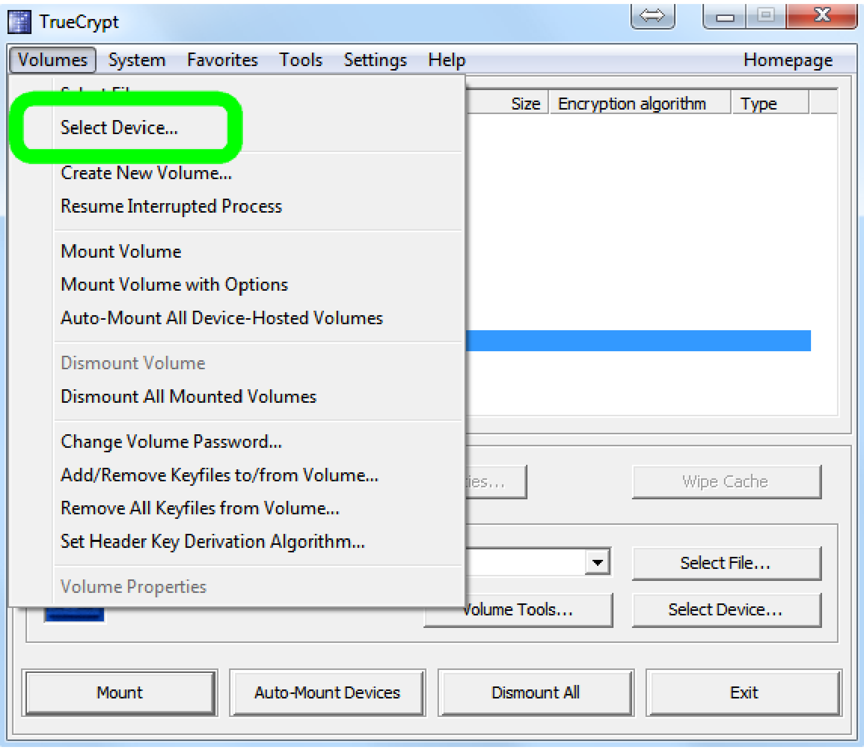
- **TrueCrypt –** Use this software if the Destination drive was encrypted with the ***TC-XTS*** cipher mode.
- **FreeOTFE –** Use this software if the Destination drive was encrypted with the ***CBC*** or ***ECB*** cipher mode.

8.3.2 Decrypting using TrueCrypt

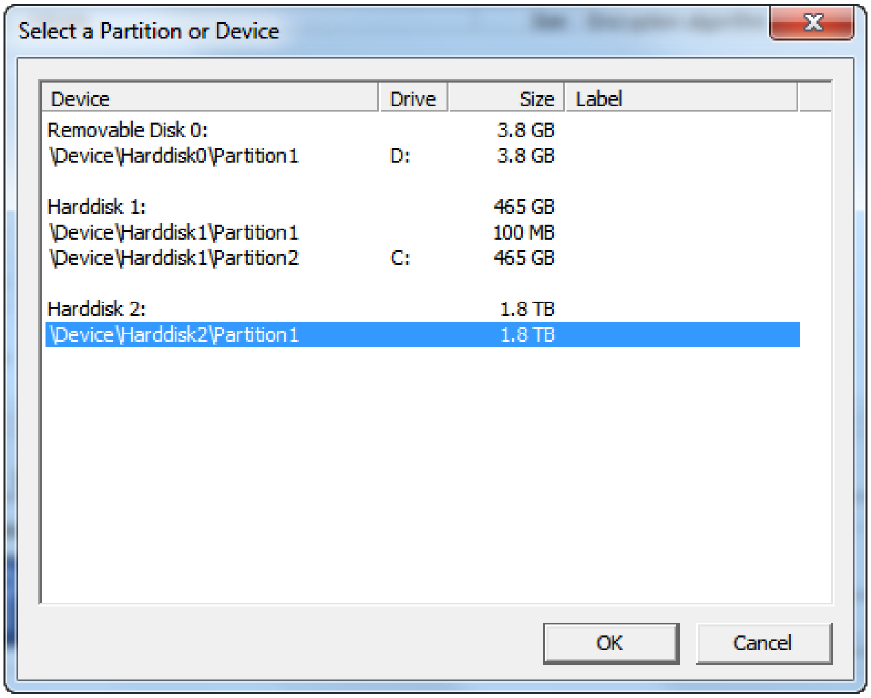
Requirements:

- TrueCrypt properly installed.
- A drive encrypted by the Falcon using the TC-XTS cipher mode connected to the computer with TrueCrypt.

1. Open TrueCrypt and select ***Volumes*** from the menu system, then click ***Select Device…***



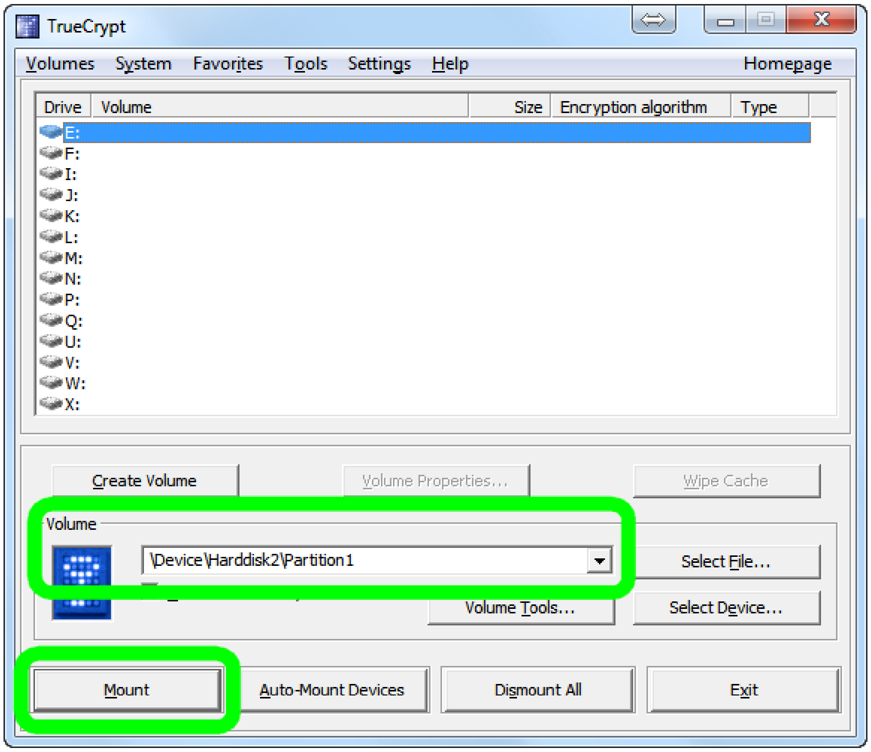
2. The ‘Select a Partition or Device’ window will appear. Select the partition of the drive. Do not select the actual drive itself. Click ***OK*** to continue.



Select a Partition or Device

Device	Drive	Size	Label
Removable Disk 0:		3.8 GB	
\Device\Harddisk0\Partition1	D:	3.8 GB	
Harddisk 1:		465 GB	
\Device\Harddisk1\Partition1		100 MB	
\Device\Harddisk1\Partition2	C:	465 GB	
Harddisk 2:		1.8 TB	
\Device\Harddisk2\Partition1		1.8 TB	

3. Verify the ***Volume*** shows the correct device and partition. Click ***Mount*** to continue.

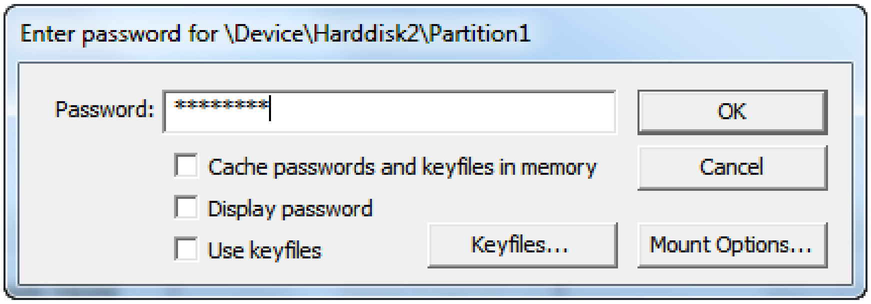


TrueCrypt

Drive	Volume	Size	Encryption algorithm	Type
E:				
F:				
I:				
J:				
K:				
L:				
M:				
N:				
P:				
Q:				
U:				
V:				
W:				
X:				

Volume: \Device\Harddisk2\Partition1

4. The password screen will appear. Enter the password used to encrypt the drive then click ***OK*** to continue.



Enter password for \Device\Harddisk2\Partition1

Password: *********

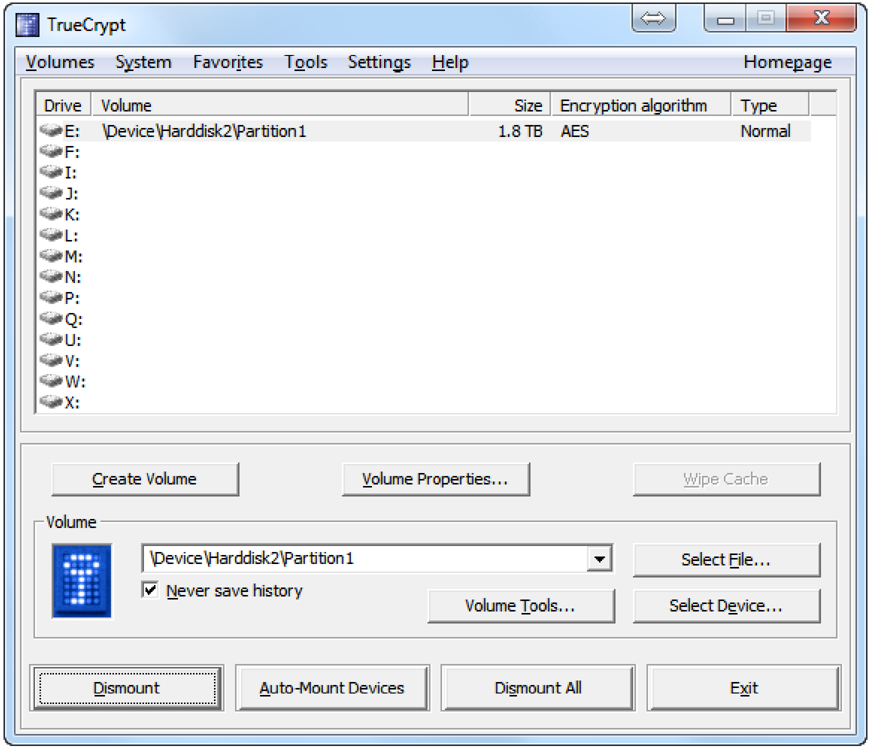
□ Cache passwords and keyfiles in memory

□ Display password

□ Use keyfiles

TrueCrypt has a setting to mount the drive as "read-only" which is a software write-block. This setting can be found by clicking ***Mount Options…*** A hardware write-block device may be used instead, if needed.

5. TrueCrypt will mount the drive and assign it a drive letter.



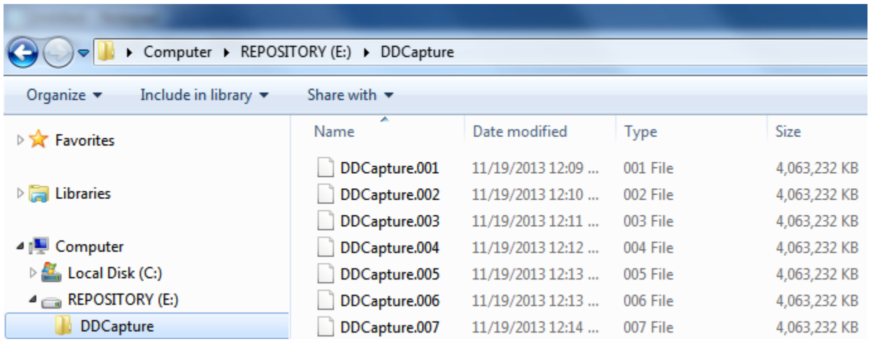
Drive	Volume	Size	Encryption algorithm	Type
E:	\Device\Harddisk2\Partition1	1.8 TB	AES	Normal
F:				
I:				
J:				
K:				
L:				
M:				
N:				
P:				
Q:				
U:				
V:				
W:				
X:				

Volume

\Device\Harddisk2\Partition1

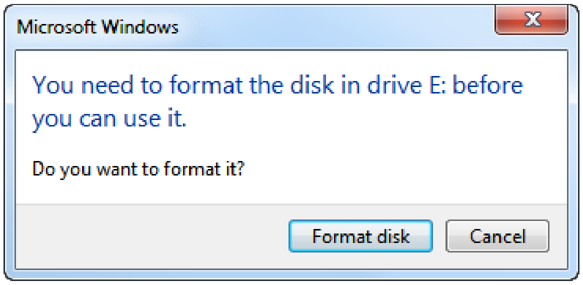
☑ Never save history

6. The Destination drive should now be accessible in Windows.



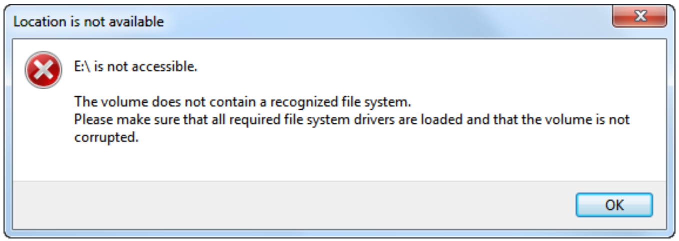
Name	Date modified	Type	Size
DDCapture.001	11/19/2013 12:09 ...	001 File	4,063,232 KB
DDCapture.002	11/19/2013 12:10 ...	002 File	4,063,232 KB
DDCapture.003	11/19/2013 12:11 ...	003 File	4,063,232 KB
DDCapture.004	11/19/2013 12:12 ...	004 File	4,063,232 KB
DDCapture.005	11/19/2013 12:13 ...	005 File	4,063,232 KB
DDCapture.006	11/19/2013 12:13 ...	006 File	4,063,232 KB
DDCapture.007	11/19/2013 12:14 ...	007 File	4,063,232 KB

If the Destination drive was formatted with the EXT4 file system, and Ext2Fsd is not installed, the following messages may appear in Windows. Make sure Ext2Fsd is installed if the Destination drive was formatted with the EXT4 file system.


Microsoft Windows

You need to format the disk in drive E: before you can use it.

Do you want to format it?


Location is not available

E:\ is not accessible.

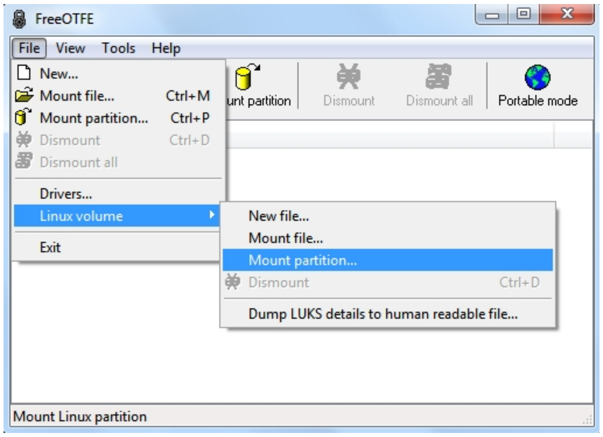
The volume does not contain a recognized file system.
Please make sure that all required file system drivers are loaded and that the volume is not corrupted.

8.3.3 Decrypting using FreeOTFE

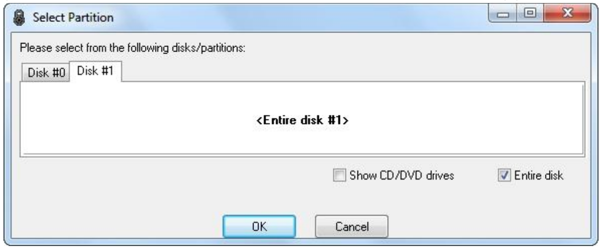
Requirements:

- FreeOTFE properly installed
- A drive encrypted by the Falcon using the CBC or ECB cipher mode connected to the computer with FreeOTFE.

1. Open FreeOTFE. In the main window, click ***File*** then ***Linux volume*** then ***Mount partition…***



2. Select the encrypted disk to mount (in this example, it is Disk #5). Place a check mark on the ***Entire disk*** option. FreeOTFE cannot read the partition table on the drive since it is encrypted at this time.

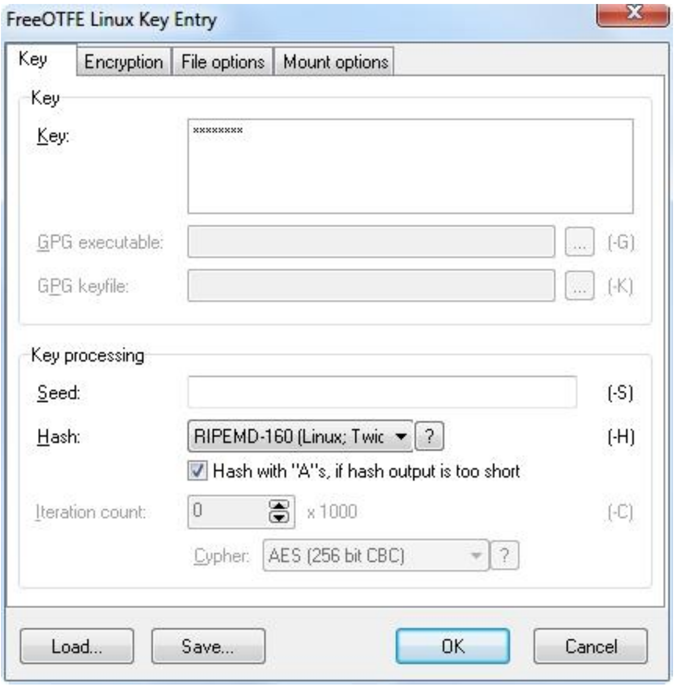


Please select from the following disks/partitions:

<Entire disk #1>

□ Show CD/DVD drives
☑ Entire disk

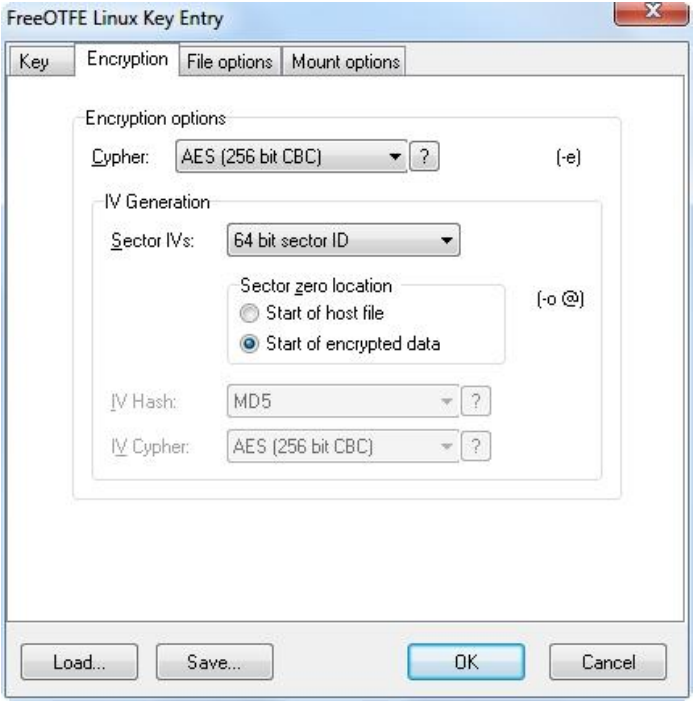
3. In the Key tab, enter the Key (password) and make sure the ***Hash*** is set to ***RIPEMD-160***.



Key: ********
GPG executable: ... (-G)
GPG keyfile: ... (-K)

Seed: (-S)
Hash: RIPEMD-160 (Linux; Twic ? (-H)
☑ Hash with "A"s, if hash output is too short
Iteration count: 0 x 1000 (-C)
Cypher: AES (256 bit CBC) ?

4. In the Encryption tab, set the ***Cipher*** to ***AES (256 bit CBC)***. Set the ***Initialization Vector (IV) generation*** method to match what was used in the ***IV Generation*** on the Falcon. In this example, "plain64' was used. In the 'Sector zero location', choose ***Start of encrypted data***.



FreeOTFE Linux Key Entry

Encryption options

Cypher: AES (256 bit CBC) (-e)

IV Generation

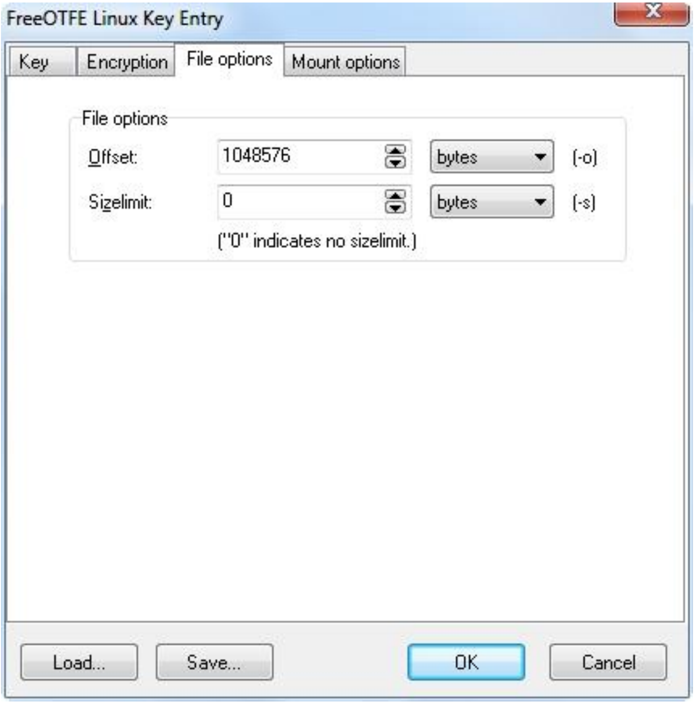
Sector IVs: 64 bit sector ID

Sector zero location (-o @)
○ Start of host file
● Start of encrypted data

IV Hash: MD5

IV Cypher: AES (256 bit CBC)

5. In the ***File options*** tab, set the ***Offset*** to 1048576. Since the Falcon uses the EXT4 file system, the offset is at 2048 sectors, or 1048576 bytes.



FreeOTFE Linux Key Entry

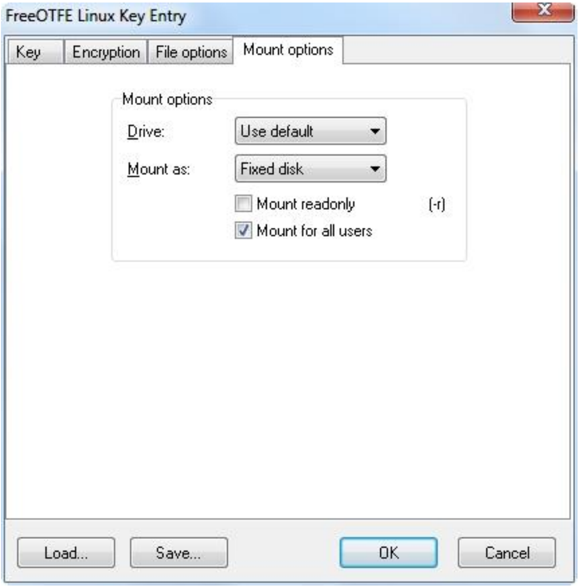
File options

Offset: 1048576 bytes (-o)

Sizelimit: 0 bytes (-s)

("0" indicates no sizelimit.)

OPTIONAL: In the ***Mount options*** tab, the disk can also be mounted with write protection. To do so, make sure the ***Mount readonly*** option is checked. Windows may not mount the drive if this option is checked. If this is the case, use a write-protect device and uncheck the ***Mount readonly*** option.



Mount options

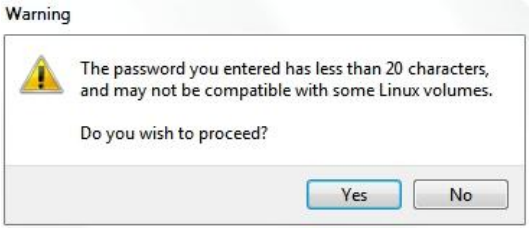
Drive: Use default

Mount as: Fixed disk

□ Mount readonly (-r)

☑ Mount for all users

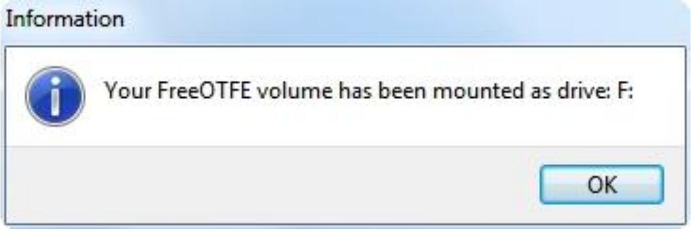
6. Click the ***OK*** button. The following warning screen may appear. Click the ***Yes*** button to continue.



The password you entered has less than 20 characters, and may not be compatible with some Linux volumes.

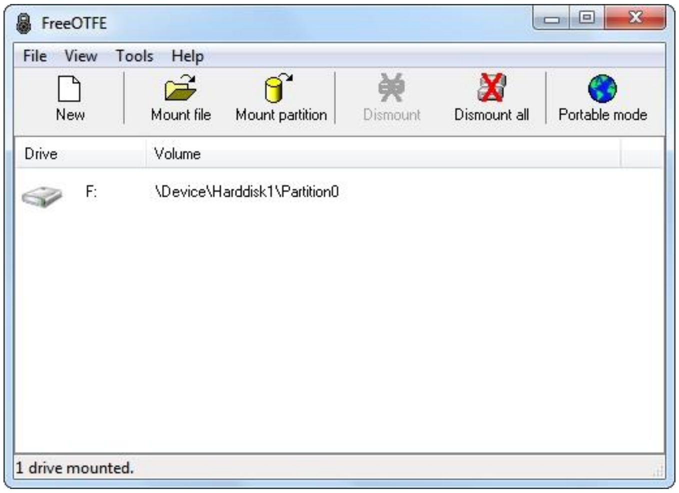
Do you wish to proceed?

7. FreeOTFE will mount the drive and assign a drive letter.



Your FreeOTFE volume has been mounted as drive: F:

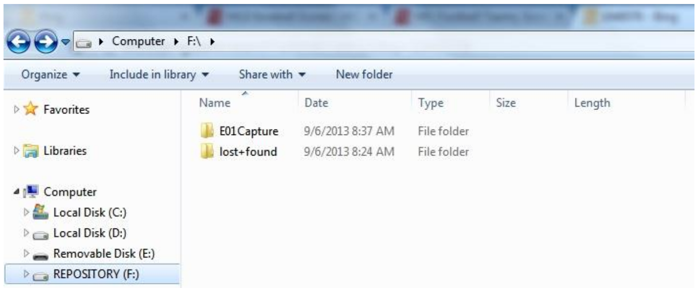
8. Click the ***OK*** button to continue. The drive should appear in the FreeOTFE window.



Drive	Volume
F:	\Device\Harddisk1\Partition0

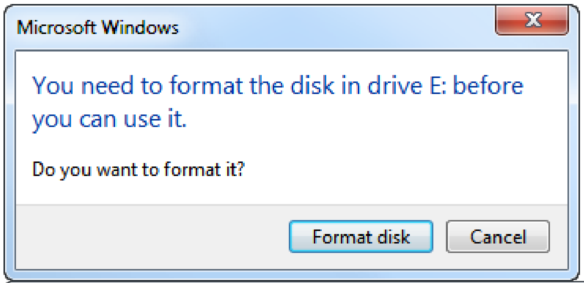
1 drive mounted.

9. The Destination drive should now be accessible in Windows.



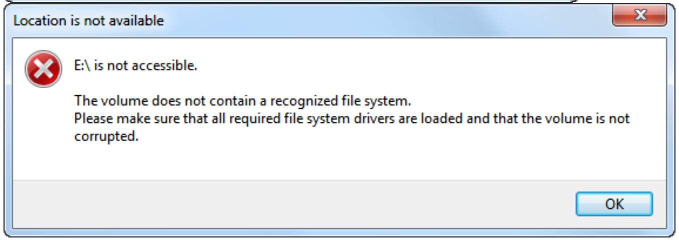
Name	Date	Type	Size	Length
E01Capture	9/6/2013 8:37 AM	File folder		
lost+found	9/6/2013 8:24 AM	File folder		

If the Destination drive was formatted with the EXT4 file system, and Ext2Fsd is not installed, the following messages may appear in Windows. Make sure Ext2Fsd is installed if the Destination drive was formatted with the EXT4 file system.



You need to format the disk in drive E: before you can use it.

Do you want to format it?



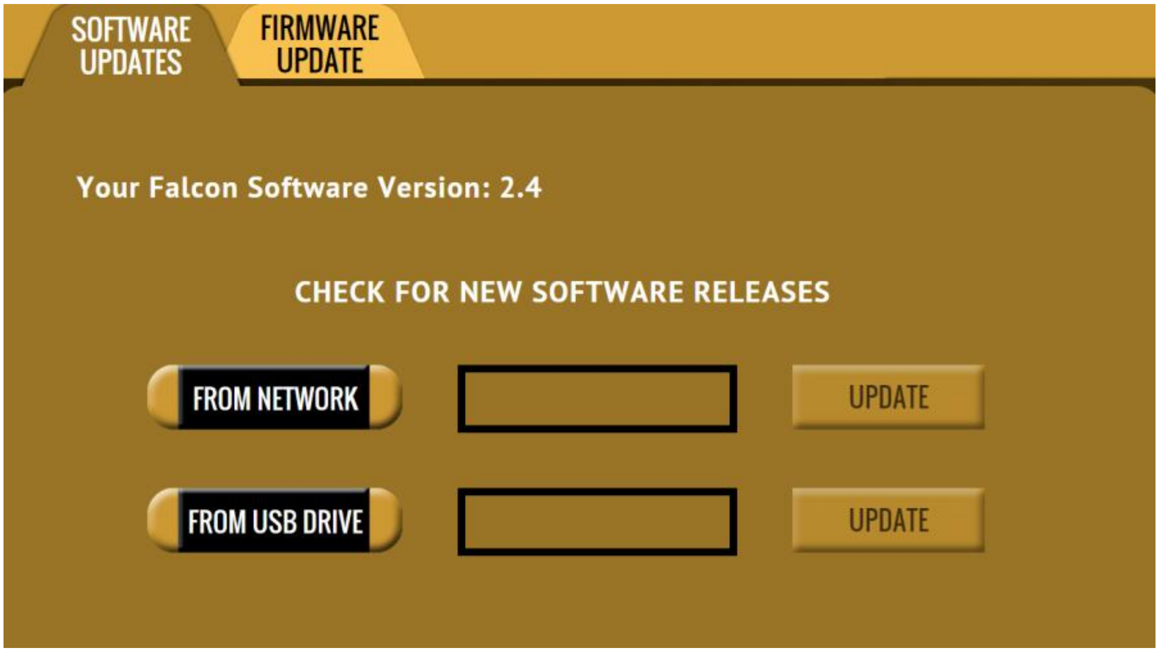
E:\ is not accessible.

The volume does not contain a recognized file system.
Please make sure that all required file system drivers are loaded and that the volume is not corrupted.

9: Updating the Falcon Software

9.0 Loading New Software

New and improved software will be released from time to time and will always be available on the Falcon support page at http://www.logicube.com/knowledge/forensic-falcon.



Your Falcon Software Version: 2.4

CHECK FOR NEW SOFTWARE RELEASES

9.1 Software Loading Instructions

There are two methods of how to update the Falcon software:

A. **FROM NETWORK –** Via the Internet through a network connection

B. **FROM USB DRIVE** – Via software file download onto a USB drive flash.

The actual software installation will take about 5 minutes. If ***FROM NETWORK*** was chosen, the total time can exceed 10 to 20 minutes (or longer) depending on Internet speeds and Internet traffic.

The most up-to-date instructions on updating the software can be found on the Falcon's support page at: http://www.logicube.com/knowledge/forensic-falcon

9.1.1 From Network – Via the web

1. Connect the Falcon to a network with Internet access. Set the proxy settings (IP settings) if necessary. Attach a network cable to the back of the Falcon.

The Falcon is DHCP enabled by default.

2. From the main menu on the Falcon, tap the down arrow twice then tap the ***Software Updates*** icon. A screen will appear showing the current version of software installed towards the top of the screen.
3. Select ***From Network***. The Falcon will check for a newer version on the web. If one is found, it will display the version on the screen and the ***Update*** icon will be selectable.
4. Tap the ***Update*** icon to begin the update. A confirmation screen will appear. Tap ***Yes*** to continue the update.
5. Do not interrupt the update process. It may take several minutes. Once completed, a 'Successful' screen will appear.
6. Reboot the Falcon by turning the unit off then back on using the Power switch in the back of the unit.
7. Verify the software version at the top of the 'Software Updates' screen.

9.1.2 From USB Drive – Via software download

The latest software can also be downloaded from Logicube's website and be placed onto a USB flash drive.

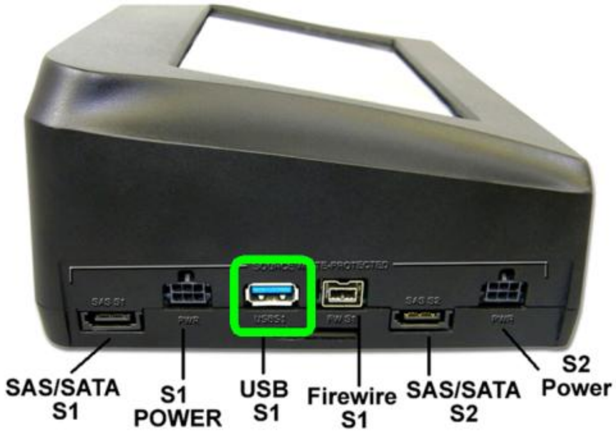
It is recommended to use an empty USB flash drive.

Download the latest software from the Falcon product support page at http://www.logicube.com/knowledge/forensic-falcon

1. Download the zip file from the download page.
2. Extract the contents of the downloaded zip file to the root of the USB flash drive (the file must not be in any folder). **Do not** connect the USB flash drive yet. The Falcon will display a message when to connect the USB drive.

If the computer being used to extract the contents of the downloaded zip file has the software WinZip, or other third party zip software, please review ***Section 9.1.2.1*** before proceeding.

3. From the main screen, tap the ***Software Updates*** icon.
4. Select From USB Drive. The Falcon will prompt for the USB drive to be connected to USB_S1.
5. Connect the USB drive to USB_S1. Falcon will then check for the version of the software on the USB drive and will display that version on the box next to the selected location.



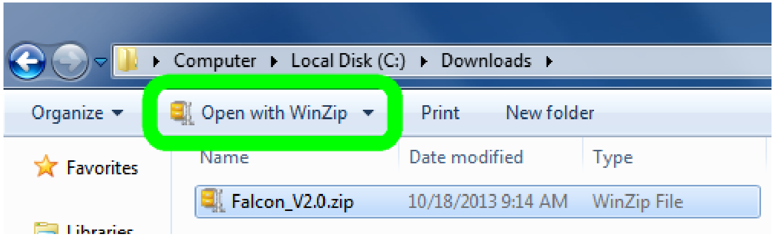
6. Tap the Update icon to begin the update. A confirmation screen will appear. Tap ***Yes*** to continue the update. Do not interrupt the update process. It may take several minutes. Once completed, a ‘Successful’ screen will appear.
7. Reboot the Falcon by turning the unit off then back on using the Power switch in the back of the unit.
8. Verify the software version at the top of the ‘Software Updates’ screen.

9.1.2.1 Extracting the software download on a computer with WinZip (or other third party zip software)

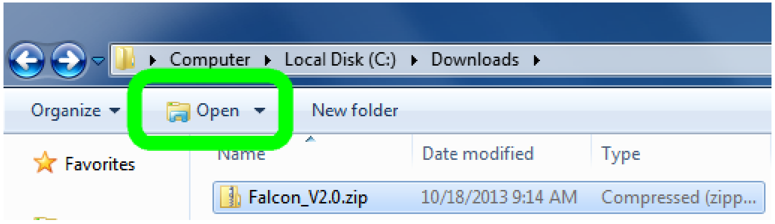
WinZip and other third party zip software may improperly extract the files required for the software update. There are compressed files within the download that need to stay compressed.

If the computer being used to extract the software download has WinZip or other third party zip software, it is highly recommended to use the built-in utility in Windows.

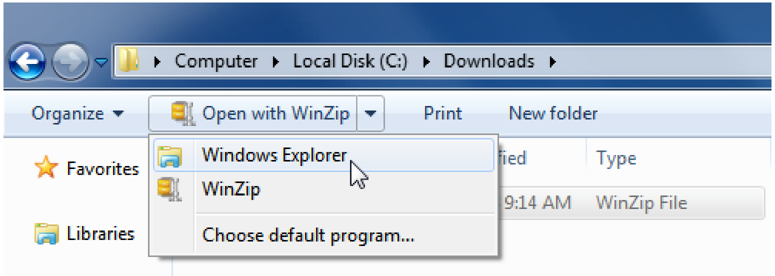
If the downloaded zip file is highlighted and WinZip is installed, there will be an option to ‘Open with WinZip’.



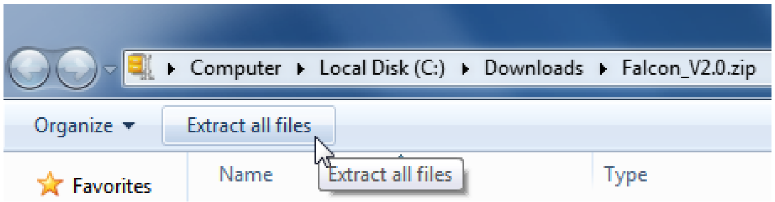
A computer without WinZip installed will have an option to ‘Open’ when the file is highlighted.



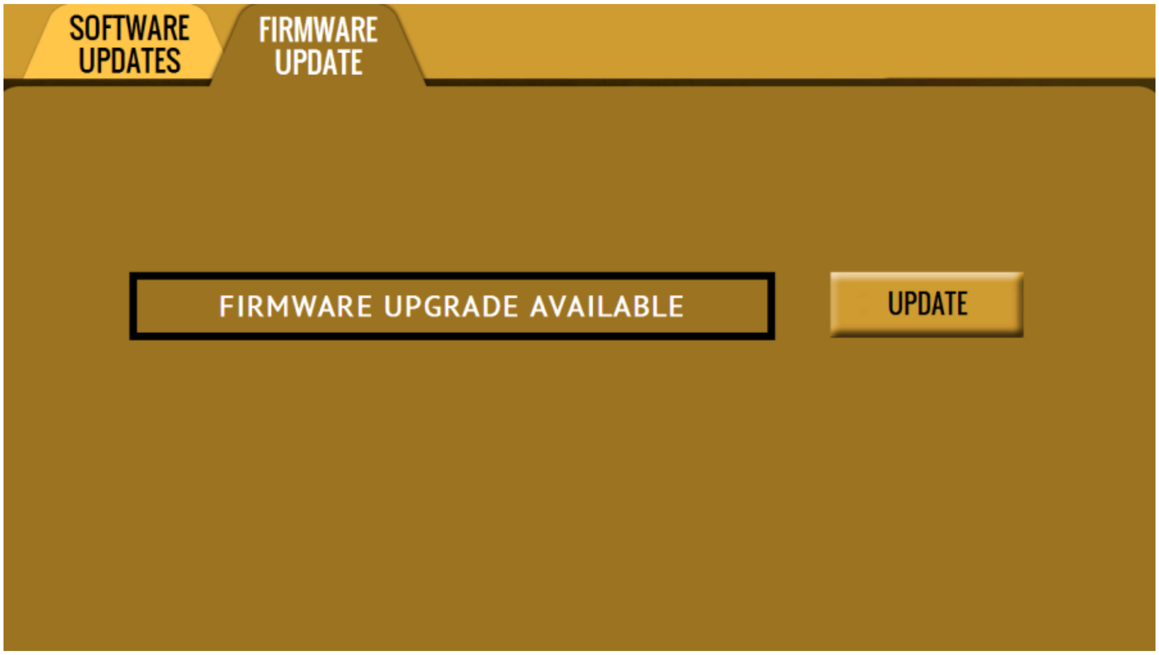
If WinZip is installed, highlight the downloaded zip file then click the arrow pointing downward next to ‘Open with WinZip’. A drop-down menu will appear. Select ***Windows Explorer***.



Windows Explorer will open the zip file and the files can be extracted using the ***Extract all files*** function to the USB flash drive. This will bypass WinZip and use the built in utility in Windows.



9.2 Firmware Loading Instructions



Some software releases may contain a firmware upgrade. The steps below outline how to check if the Falcon requires a firmware upgrade:

1. After the software is updated on the Falcon, from the main menu, tap the down arrow twice then tap the ***Software Updates*** icon.
2. Tap the "Firmware Update" page. One of two screens will appear:
   a. ***FIRMWARE UPGRADE AVAILABE –*** Tap the ***Update*** icon. A message will appear: "FIRMWARE UPDATE COULD TAKE UP TO A FEW MINUTES TO COMPLETE; PLEASE DO NOT INTERRUPT POWER DURING THIS TIME. ON COMPLETION THE UNIT WILL AUTO-RESTART AND CONFIRM THE UPDATE." Tap the ***OK*** icon to start the firmware update process.

      When the ***OK*** icon is tapped, the screen may appear to do nothing. Do not keep tapping the ***OK*** icon. The firmware update will take no more than 60 seconds. When the firmware update finishes, the Falcon will reboot automatically.

   b. ***FIRMWARE UPGRADE NOT AVAILABLE –*** This message will appear if the device does not require a firmware update. No further action is necessary if this message appears.

10: Remote Operation

10.0 Introduction

The Falcon comes with a gigabit network connection in the back of the unit. Connecting the Falcon to a network allows remote access to the Falcon from any computer within the same network.

The Falcon is configured for DHCP by default. See **Section 10.5** for instructions on how to configure the Falcon with a Static IP address.

The Falcon is setup with a Zero Configuration Network (Zeroconf). There are two ways to access the Falcon:

- Web interface – A graphical interface using an Internet browser where the screens are shown exactly the way they appear on the Falcon
- Command Line Interface (CLI) – A text only command line interface that can be accessed one of two ways:
    i. Telnet (via a network connection)
    ii. SSH (Secure Shell via a network connection)

BROWSER COMPATIBILITY: Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer 10 are recommended. Other versions of Internet Explorer may not compatible.

10.1 Web Interface

Using a web browser, go to the IP address or the name of the Falcon with its serial number. Both IP address and serial number can be found by going to the ***Statistics*** screen on the Falcon. For example, browse to http://192.168.1.100 or http://Falcon-XXXXXX/ where XXXXX is the 6 digit serial number of the Falcon. The Falcon's web interface will appear on the browser screen. All screens and operations available on the Falcon will be available on the browser.

On some browsers or Operating Systems, the Falcon will need to be accessed by browsing to http://Falcon-XXXXXX.local/.

The Falcon can be controlled by clicking on the icons appearing on the browser window.

10.2 Command Line Interface (CLI)

The Falcon also has a CLI, or Command Line Interface. This interface has no graphical content and is all command line (text) based and is for advanced users who have knowledge of command line functions. This type of connection requires a Telnet or SSH client. There are several telnet and SSH clients available from different software companies. Microsoft Windows also has a built-in Telnet client that can be used.

- Windows XP has a built-in Telnet client.
- Windows Vista, 7, 8, and 8.1 have a built-in Telnet client but is not installed by default. Installing the Telnet client may require the assistance of a Network or Systems Administrator. Other third party Telnet programs are available.
- All versions of Windows do not have a built-in SSH client.
- The instructions in this manual only refer to the clients that come with Windows. There are many third party Telnet or SSH clients available. For instructions and support for third party clients, please contact the software manufacturer.

10.3 Installing the Telnet client in Windows Vista, 7, 8, or 8.1

By default, the Telnet Client is not installed with Windows, but it can be installed it by following the steps below:

1. Open ***Control Panel*** and select either ***Programs & Features*** or ***Programs***.
2. Click ***Turn Windows features on or off***. If a prompt for an administrator password or confirmation, type the administrator password or provide confirmation (A Network or Systems Administrator may be required for administrator access).
3. In the Windows Features dialog box, select the Telnet Client check box.
4. Click OK. The installation might take several minutes.

10.3.1 Connecting via Telnet

Once the Telnet client is installed, follow the steps below to connect using the Windows Telnet client.

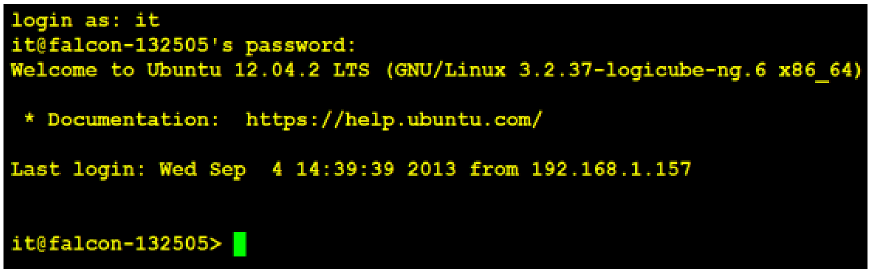
1. Connect the Falcon to the network by attaching a network cable (CAT 6 type) to the RJ45 connector in the back of the Falcon.
2. Turn the Falcon on and allow it to boot up completely.
3. Open the Telnet client.
   a. For Windows XP, click ***Start > Run.*** The Run window should appear. Type ***telnet*** in the Open: field and press Enter. The Telnet window should appear.

b. For Windows Vista or 7, click ***Start*** and in the ***Search*** field, type ***Telnet***. Telnet should appear in search results.

4. Type ***open*** followed by the IP address or name of the Falcon. For example ***open 192.168.1.100*** or ***open Falcon-XXXXXX*** where XXXXXX is the 6 digit serial number of the Falcon, then press Enter. The Falcon login screen should appear.

   Note: On some Operating Systems, the Falcon will need to be accessed by opening Falcon-XXXXXX.local.

5. Login with the username "***it***" (without the quotes) and the password "***it***" (without the quotes).
6. The following prompt should appear in the Telnet window:



```
login as: it
it@falcon-132505's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.2.37-logicube-ng.6 x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Wed Sep  4 14:39:39 2013 from 192.168.1.157


it@falcon-132505>
```

7. The Falcon can now be configured or managed via the command line interface.

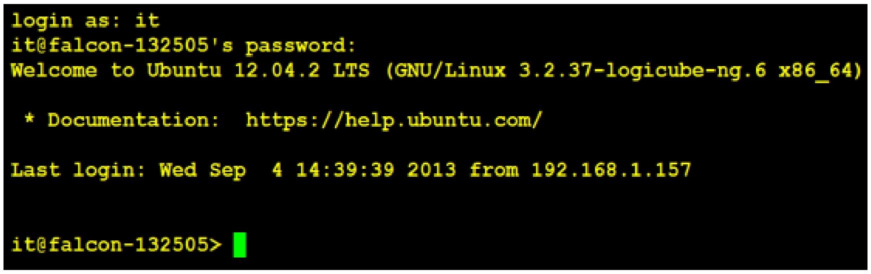
10.3.2 Connecting via SSH

Connecting to the Falcon via SSH (Secure Shell) is very similar to connecting via Telnet. Since Windows does not have a built-in SSH client, a third party SSH client will need to be downloaded and installed to connect via SSH. For instructions and support on how to use third party SSH clients, please contact the SSH client's manufacturer.

1. Connect the Falcon to the network by attaching a network cable (CAT 6 type) to the RJ45 connector in the back of the Falcon.
2. Turn the Falcon on and allow it to boot up completely.
3. Open the SSH client and select an SSH connection.
4. Connect to the Falcon either by IP address or by name. The name of the Falcon will be **Falcon-*XXXXXX*** where XXXXXX is the serial number of the Falcon).

   On some Operating Systems, the Falcon will need to be accessed by opening Falcon-XXXXXX.local.

5. Login with the username "***it***" (without the quotes) and the password "***it***" (without the quotes).
6. The following prompt should appear in the SSH window:



```
login as: it
it@falcon-132505's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.2.37-logicube-ng.6 x86_64)

 * Documentation:  https://help.ubuntu.com/

Last login: Wed Sep  4 14:39:39 2013 from 192.168.1.157

it@falcon-132505>
```

7. The Falcon can now be configured or managed via the command line interface.

10.4 Zero Configuration Networking (Zeroconf)

The Falcon has the capabilities for Zero Configuration Networking (Zeroconf). Zeroconf allows devices to automatically create a usable computer network based on the Internet Protocol Suite (TCP/IP).

For example, when the Falcon is connected (connected via a network cable) directly to a Windows based computer that is DHCP enabled, both the Falcon and the Windows based computer will automatically configure themselves to be seen by each other using TCP/IP.

10.5 Configuring the Falcon with a static IP address

The Falcon is DHCP enabled by default. Some networks do not support DHCP and require a static IP address. The Falcon can be configured with a static IP address and needs to be connected to a network with DHCP first.

10.5.1 Step-by-step instructions – Static IP address

1. Connect the Falcon to a network with DHCP.
2. Turn the Falcon on. The Falcon should automatically assign itself an IP address that the Windows computer can see. Go to the ***Statistics*** screen on the Falcon and take a look at the HostName and IPAddress.
3. Using Telnet or SSH, connect to the Falcon. Instructions on how to connect via Telnet or SSH can be found in **Section 10.3.1 or 10.3.2**.
4. Once logged in to the Falcon via CLI, follow these steps to set the IP address to a static IP:
    a. From the main prompt, type ***command*** then press the enter key.
    b. Type ***config*** then press the enter key.
    c. Type ***net del -n eth0*** to delete the current network configuration.

d. The following information is required: a static IP, the netmask, network gateway, the network nameserver, the domain. For example:
   i. IP Address: 192.168.1.123
   ii. Netmask: 255.255.255.0
   iii. Gateway: 192.168.1.10
   iv. Nameserver: 192.168.1.10 (typically the same as the gateway unless the network has a specific nameserver IP.
   v. Domain: LG

> Networks are configured differently and the necessary settings may require the assistance of a Network or Systems Administrator.

e. Based on the info above, the example for this line will be to type (case sensitive): ***net add -n eth0 -t static -a 192.168.1.143 -m 255.255.255.0 -g 192.168.1.1 -N 192.168.1.1 -d lg*** then press the enter key.

f. The Falcon should respond with the following: Command (DbNetworkConfig) Successful

g. Now we need to save the configuration. Type ***db save staticip.db*** then press the enter key. A "Successful" message should appear.

h. Type ***db load staticip.db*** to load the database configuration.

i. Perform a full shut down on the Falcon. Wait about 30 seconds then turn the Falcon back on. The Falcon should load the new configuration. The IP address can be checked by going to the Statistics screen.

10.6 Copying User Profiles/Configurations from one Falcon to another

User profiles can be copied from one Falcon to another using the Command Line Interface (CLI). The Falcon units must be on the same network and all User Profiles/Configurations will be copied over. This can be useful when non-default profiles/configurations are setup, and multiple Falcons need to have the same profiles/configurations. Instead of configuring each Falcon one at a time, all Falcons can have the same profiles/configurations with a few simple commands.

10.6.1 Step-by-step – Copying User Profiles/Configurations

1. Set up any (or all) User Profiles/Configurations on one Falcon. Make sure each profile/configuration is saved, and load the profile/configuration that should be loaded during each time the Falcon is turned on.

2. Connect two or more Falcons to a network with DHCP. One of the Falcons connected should be the one with the profiles/configurations already set up.
3. Using Telnet or SSH to the Falcon with the profiles/configurations already set up, connect to the Falcon's Command Line Interface (CLI) via Telnet or SSH (see sections 10.3.1 and 10.3.2 for more information on connecting via Telnet or SSH).
4. Once connected via CLI, log in with the following credentials:
    a. Username: ***it***
    b. Password: ***it***.
5. From the main prompt, type ***command*** then press the Enter key.
6. Type ***config*** then press the Enter key.
7. Type ***db list*** then press the Enter key. This will show all the profiles/configurations to on this Falcon unit. Make sure that these are the profiles/configurations that need to be copied to the other Falcons.
8. Type ***db push xxx.xxx.xxx.xxx*** where xxx is the IP address of the Falcon that the profiles/configurations will be copied to (for example, db push 192.168.1.101) then press the Enter key. The profiles/configurations on the first Falcon will be copied to the other Falcon. This may take a few minutes depending on network speeds, and the number of configurations to copy. When the process is finished, the screen will show "…Done" and the CLI prompt will appear.
9. Repeat step 8 to copy the profiles/configurations to other Falcon units.
10. When finished, reboot all the Falcons where the profiles/configurations were copied to. They should boot up with the same profiles/configuration set to load and all other saved profiles/configurations.

11: Viewing Source and Destination Drives over a Network

11.0 Overview

The contents of drives connected to any Source or Destination position on the Falcon can be viewed over a network.

To view Source the contents of a Source drive over a network, an iSCSI initiator is required. Windows Vista, 7, 8, and 8.1 have a built-in iSCSI initiator located in the Administrative Tools section of the Control Panel. Windows XP does not have a built-in iSCSI initiator. Microsoft has a separate download for the iSCSI initiator for Windows XP and can be found by searching Microsoft's website for ***iscsi initiator***. No data can be written or deleted to the drives.

Contents of a Destination drive can be viewed over a network using built-in file explorers/viewers. Contents of Destination drives viewed over a network are write-protected.

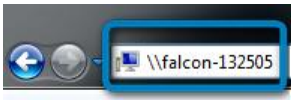
11.1 Viewing Source or Destination drives over the network using SMB

Contents of a Source or Destination drive can be viewed over a network using built-in file explorers/viewers like Windows Explorer. Contents of Source drives viewed over a network are write-protected.

Drives connected to the Source ports (SAS_S1, SAS_S2, USB_S1, and FW_S1) – Drives connected to the Source ports are always write-protected. Using the File Browser function will not alter the drive or its contents in any way.

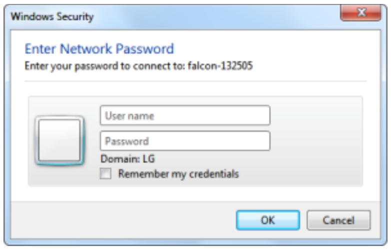
11.1.1 Step-by-step – Viewing Source or Destination drives

1. Connect the Falcon directly to a computer (using a network cable) or to a network.
2. On the computer (on the same network), open Windows Explorer and open the Falcon's IP address or the hostname of the Falcon with its serial number. Both IP address and serial number can be found by going to the ***Statistics*** screen on the Falcon. For example, browse to \\192.168.1.100 or \\falcon-XXXXXX where XXXXX is the 6 digit serial number of the Falcon.

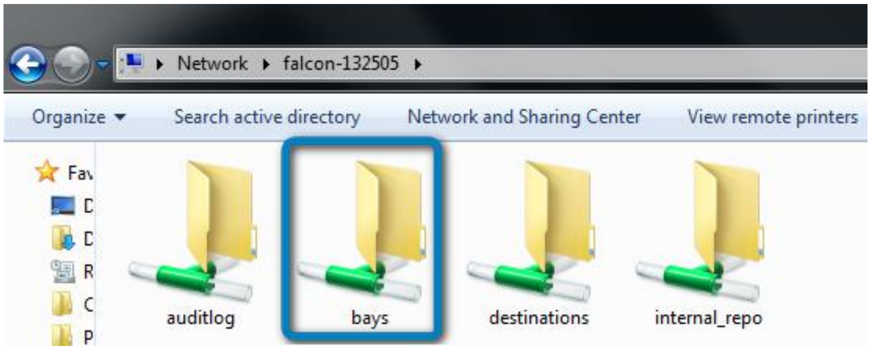


\\falcon-132505

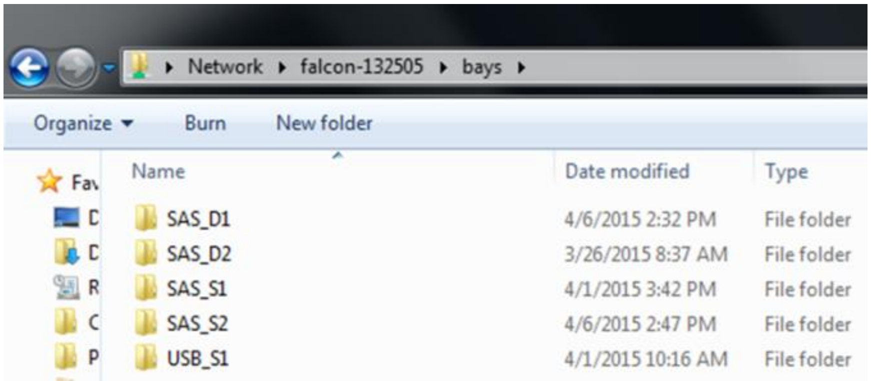
3. A window may appear asking you to enter password to connect to the Falcon. Enter the following information:
    - **a.** User name: ***it***
    - **b.** Password: ***it***



4. A folder called ***bays*** will be shown in Windows Explorer.

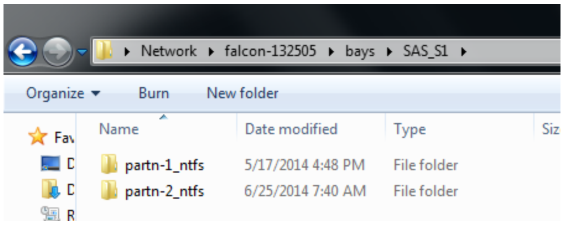


5. Go into the ***bays*** folder and select the connected Destination drive. For example, ***sas-d2***.

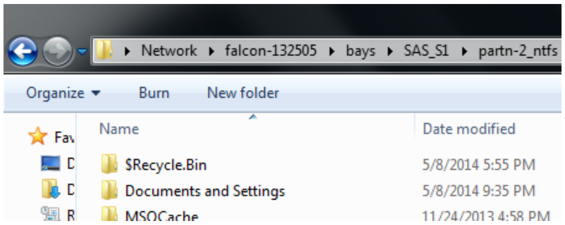


Name	Date modified	Type
SAS_D1	4/6/2015 2:32 PM	File folder
SAS_D2	3/26/2015 8:37 AM	File folder
SAS_S1	4/1/2015 3:42 PM	File folder
SAS_S2	4/6/2015 2:47 PM	File folder
USB_S1	4/1/2015 10:16 AM	File folder

6. The contents of the drive will be shown.



Name	Date modified	Type	Siz
partn-1_ntfs	5/17/2014 4:48 PM	File folder	
partn-2_ntfs	6/25/2014 7:40 AM	File folder	



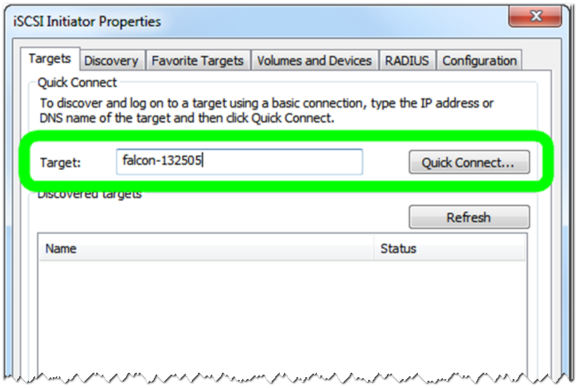
Name	Date modified
$Recycle.Bin	5/8/2014 5:55 PM
Documents and Settings	5/8/2014 9:35 PM
MSOCache	11/24/2013 4:58 PM

11.2 Viewing Source drives over the network using iSCSI

An iSCSI initiator must be configured to view the contents of Source drives over a network. Although there are many iSCSI initiators available, these next sections will discuss configuring Microsoft's iSCSI initiator in Windows.

11.2.1 Configuring the iSCSI initiator – Windows 7, 8, and 8.1

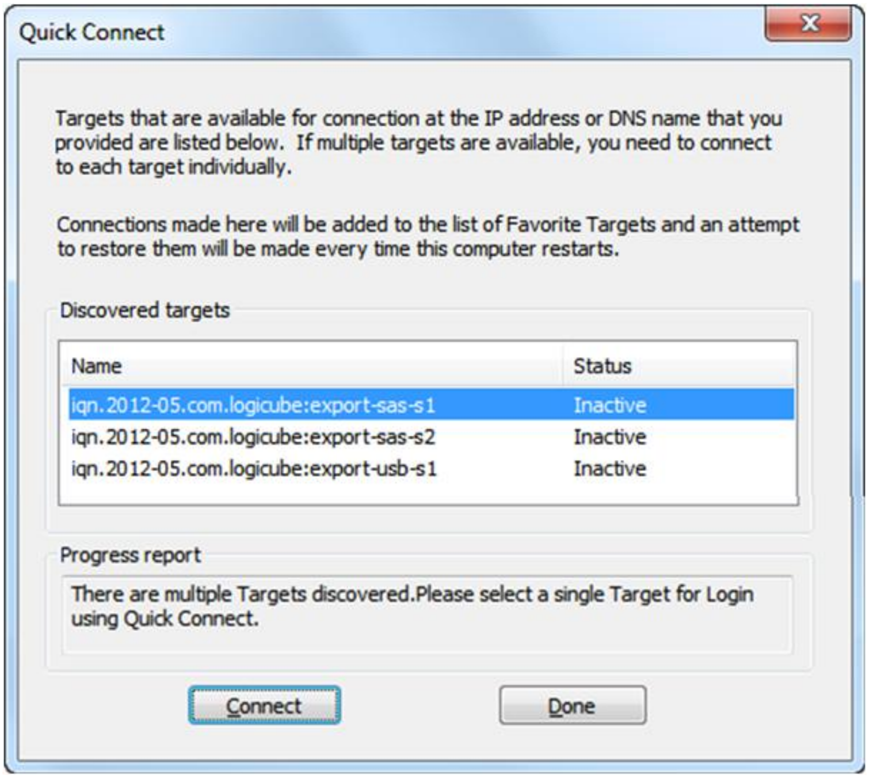
1. Open the iSCSI initiator. In the ***Target*** tab, enter the Falcon's host name or IP address in the ***Target*** field. Click the ***Quick Connect*** button to continue.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target: falcon-132505

2. The Quick Connect window will appear and any drives connected to the Source ports of the Falcon will appear on the list of discovered targets. Highlight the drive to view, then click ***Connect***.



Targets that are available for connection at the IP address or DNS name that you provided are listed below. If multiple targets are available, you need to connect to each target individually.

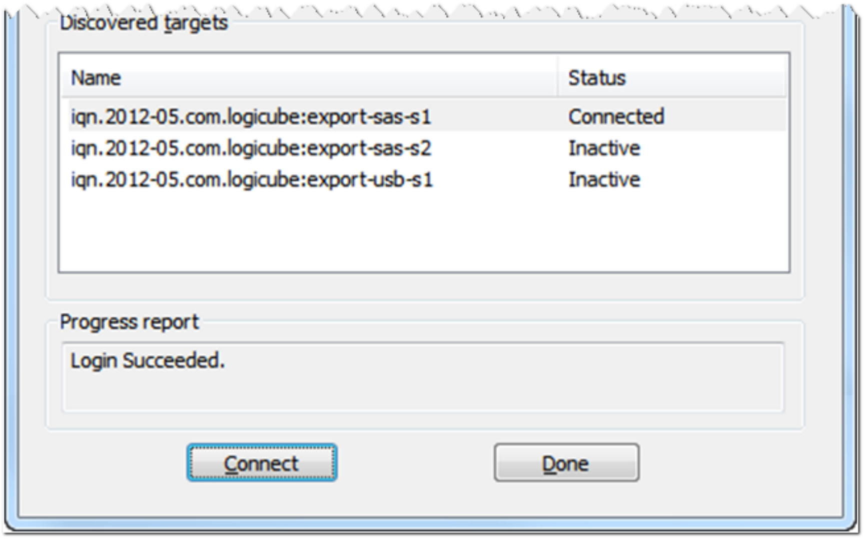
Connections made here will be added to the list of Favorite Targets and an attempt to restore them will be made every time this computer restarts.

Name	Status
iqn.2012-05.com.logicube:export-sas-s1	Inactive
iqn.2012-05.com.logicube:export-sas-s2	Inactive
iqn.2012-05.com.logicube:export-usb-s1	Inactive

There are multiple Targets discovered.Please select a single Target for Login using Quick Connect.

If only one drive is connected to the Falcon, the iSCSI initiator will automatically connect the drive, and step 3 is not necessary.

3. The selected drive status will change to ***Connected***. Repeat step 2 for all other drives to be viewed. Click ***Done*** when finished.



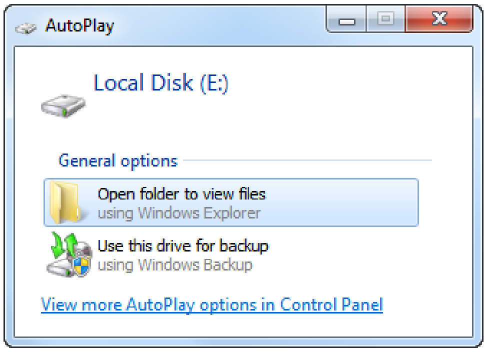
Discovered targets

Name	Status
iqn.2012-05.com.logicube:export-sas-s1	Connected
iqn.2012-05.com.logicube:export-sas-s2	Inactive
iqn.2012-05.com.logicube:export-usb-s1	Inactive

Progress report

Login Succeeded.

4. Windows will attempt to mount the drive. If it contains a file system recognized by Windows, it will automatically assign a drive letter for each recognized partition and the contents can be viewed in Windows. This process may take several minutes depending on several factors including drive size, computer specifications, and network speeds.



AutoPlay

Local Disk (E:)

General options

Open folder to view files
using Windows Explorer

Use this drive for backup
using Windows Backup

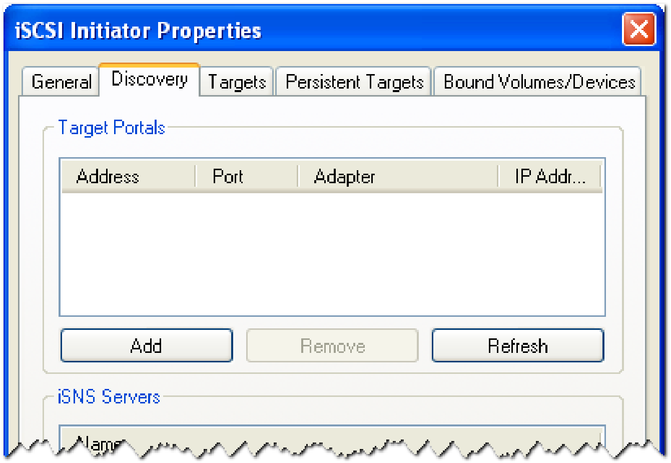
View more AutoPlay options in Control Panel

If Windows does not recognize the file system on the drive (EXT, HFS, etc.) it will not be mounted and no drive letter will be assigned.

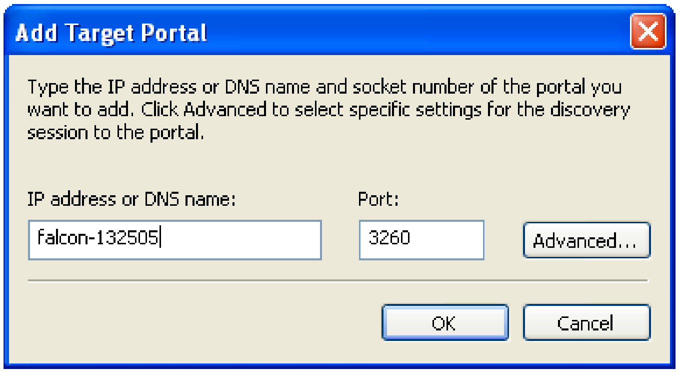
If the drive is greater than 2TB, Windows may not properly recognize the drive or its contents. For more information, please see Microsoft KB Article ID: 2581408: Windows support for hard disks that are larger than 2 TB. This can also be searched with the keyword: KB2581408

11.2.2 Configuring the iSCSI initiator – Windows XP

1. Open the iSCSI initiator. In the ***Discovery*** tab, click the ***Add*** button.



2. The Add Target Portal window will appear. Enter the Falcon's hostname or IP address. Leave the port set to 3260 then click ***OK***.

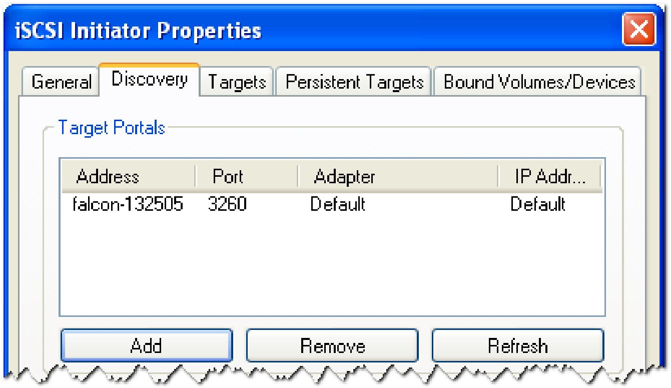


Type the IP address or DNS name and socket number of the portal you want to add. Click Advanced to select specific settings for the discovery session to the portal.

IP address or DNS name: falcon-132505

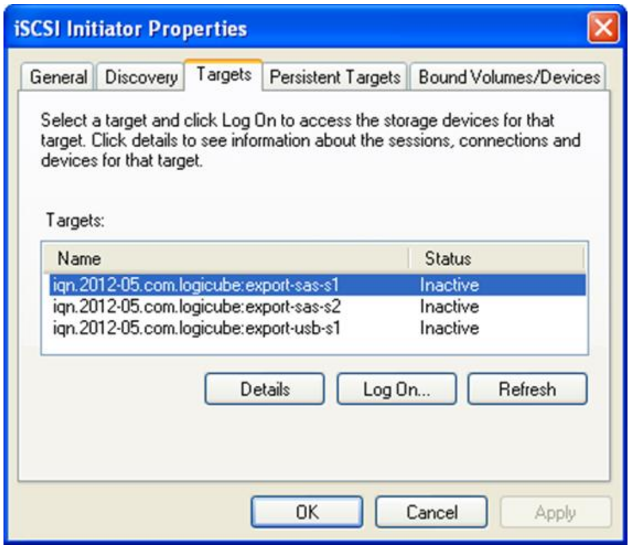
Port: 3260

3. The Falcon will be added to the Target Portals list. Click the ***Targets*** tab to select which drive to view.



Address	Port	Adapter	IP Addr...
falcon-132505	3260	Default	Default

4. In the Targets tab, any drives connected to the Source ports of the Falcon will appear on the list of targets. Highlight the drive to view, then click ***LogOn***.

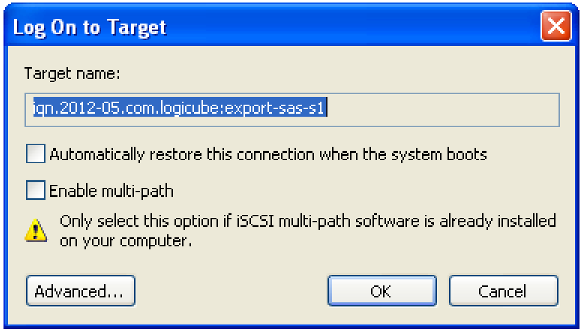


Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

Targets:

Name	Status
iqn.2012-05.com.logicube:export-sas-s1	Inactive
iqn.2012-05.com.logicube:export-sas-s2	Inactive
iqn.2012-05.com.logicube:export-usb-s1	Inactive

5. A Log on to Target window will appear. Click ***OK*** to continue.



Target name:

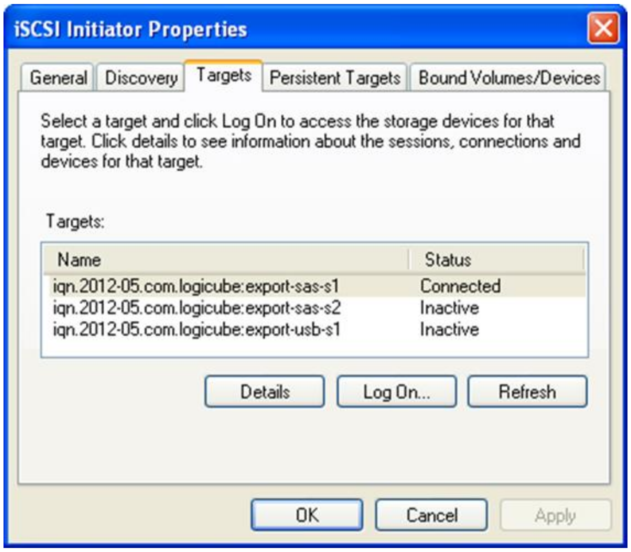
iqn.2012-05.com.logicube:export-sas-s1

□ Automatically restore this connection when the system boots

□ Enable multi-path

⚠ Only select this option if iSCSI multi-path software is already installed on your computer.

6. The selected drive status will change to ***Connected***. Repeat steps 4 and 5 to view other drives. Click ***OK*** when finished.



Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

Targets:

Name	Status
iqn.2012-05.com.logicube:export-sas-s1	Connected
iqn.2012-05.com.logicube:export-sas-s2	Inactive
iqn.2012-05.com.logicube:export-usb-s1	Inactive

7. Windows will attempt to mount the drive. If it contains a file system recognized by Windows, it will automatically assign a drive letter for each recognized partition and the contents can be viewed in Windows. This process may take several minutes depending on several factors including drive size, computer specifications, and network speeds.

> If Windows does not recognize the file system on the drive (EXT, HFS, etc.) it will not be mounted and no drive letter will be assigned.
>
> If the drive is greater than 2TB, Windows may not properly recognize the drive or its contents. For more information, please see Microsoft KB Article ID: 2581408: Windows support for hard disks that are larger than 2 TB. This can also be searched with the keyword: KB2581408

12: Optional Adapters

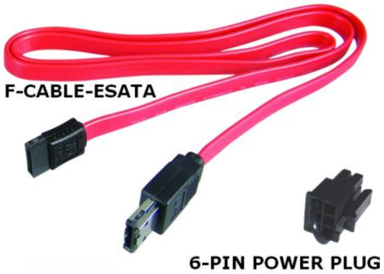
12.0 Introduction

Logicube has many different adapters that allow the imaging of almost any drive. This chapter lists the available optional adapters that can be used with the Falcon.

12.1 mSATA (mini-SATA) Drives

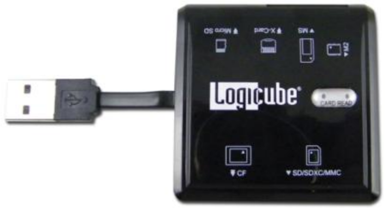
mSATA (mini-SATA) drives can be connected using the adapter shown above. This mSATA adapter has a standard SATA connector that can connect to the Falcon using the standard SATA cables included.

12.2 eSATA Drives



eSATA drives can be connected using Logicube's eSATA cable. Connect the SATA end of the eSATA cable to the Falcon and connect the eSATA end of the cable to the eSATA drive. Power to the eSATA drive should come with the drive (typically some type of external AC adapter or power cable).

12.3 Flash Memory Reader



Flash memory cards can be connected using the adapter shown above.

Third party multi-card readers are not supported and may not work with the Falcon.

The multi-card reader supports the following formats:

- CF (CompactFlash)
- SD/SDXC/MMC
- Micro SD
- Memory Stick (MS)
- Memory Stick Duo (M2)
- X-Card

Attach only one flash memory card to the multi-card reader at a time.

12.4 USB 3.0 to SATA Adapter

Logicube has qualified a USB 3.0 to SATA Adapter for use with the Falcon. This adapter provides the capability to connect SATA drives to the USB 3.0 ports on the Falcon and uses a USB 3.0 to SATA converter. USB 3.0 is a new technology and USB 3.0 controller manufacturers may have variations in device designs that have inconsistent adherence to USB 3.0 specifications. This adapter and other USB 3.0 enclosures may experience communication disruption between devices. If the adapter is not detected properly we have found that using a USB 3.0 hub may stabilize and regulate the communication between the Adapter or USB 3.0 enclosure, and the Falcon, allowing the device to be detected properly. For information on the USB 3.0 hub, please see **Section 12.5**.

12.5 USB 3.0 Hub

Some USB 3.0 is a new technology and USB 3.0 controller manufacturers may have variations in device designs that have inconsistent adherence to USB 3.0 specification. This may result in non-detection of the USB 3.0 device on certain equipment (including desktops, laptops or the Falcon). If a USB 3.0 device cannot be detected on the Falcon USB ports we have found that using a USB 3.0 hub may stabilize and regulate the communication between the USB 3.0 device and the Falcon, allowing the device to be detected properly. We have identified and qualified a USB 3.0 hub which is available as an option.

13: SCSI Module

13.0 Introduction

The optional Falcon SCSI Module expands the capability of the Falcon by providing support for imaging from and to SCSI hard drives. The SCSI module can connect to 68-pin SCSI drives natively. Optional adapters are available for use with 80-pin and 50-pin SCSI drives.

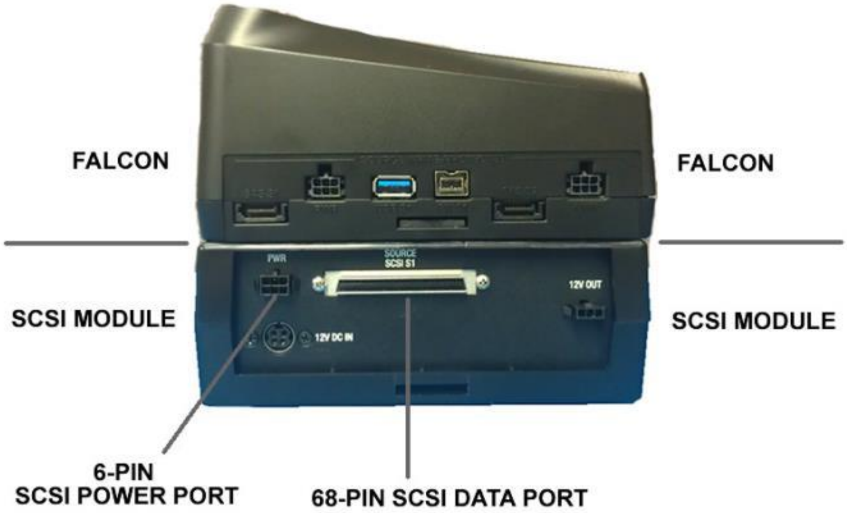
The Falcon SCSI module provides 1 SCSI write-protected Source port and 1 SCSI Destination port.

It supports all of the Falcon features including encryption, wipe, task macro, drive spanning, logs, parallel imaging, concurrent image+verify, and multi-tasking.

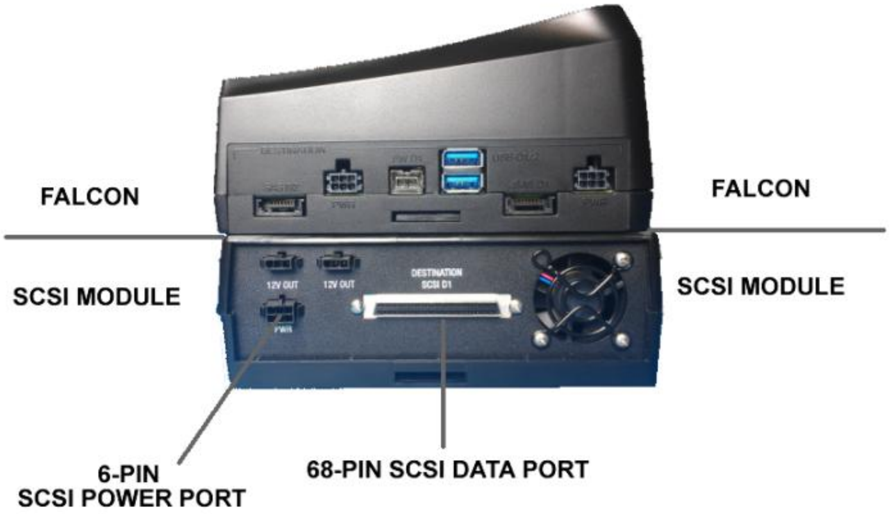
In the box:

- Power supply & power cord
- 2 SCSI drive data cables (CBL-031A)
- 2 SCSI drive power cables (CBL-EXT-PWR-04)
- Optional 50-pin and 80-pin SCSI adapters are available.

FALCON WITH SCSI MODULE
LEFT SIDE (SOURCE) VIEW



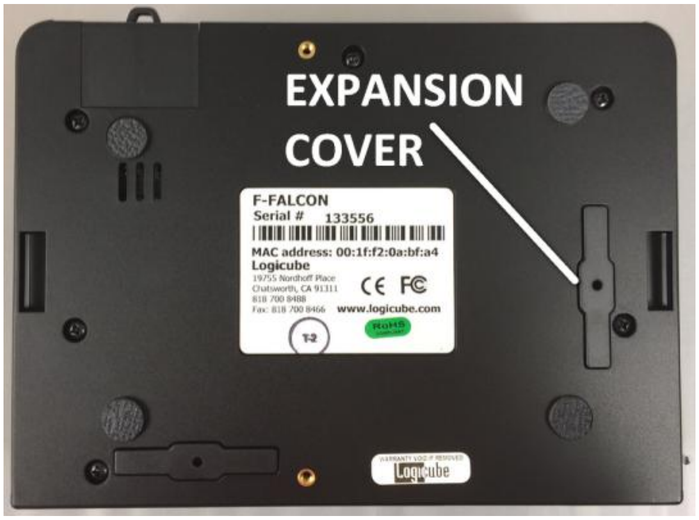
FALCON WITH SCSI MODULE
RIGHT SIDE (DESTINATION) VIEW



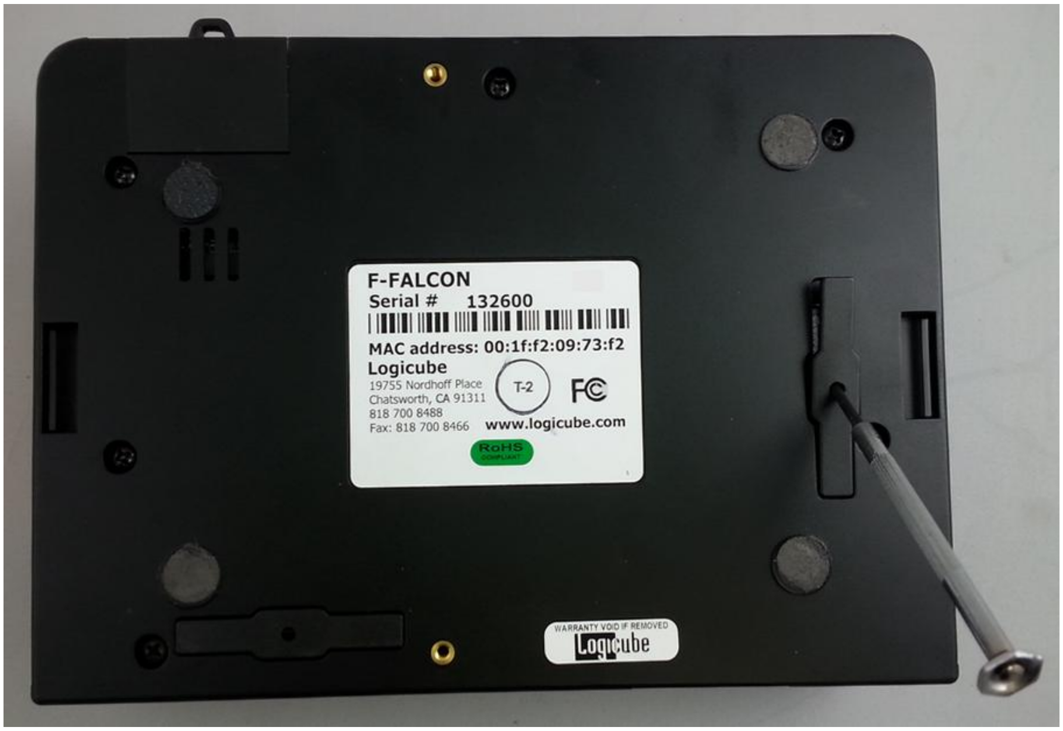
13.1 Instructions - How to attach the SCSI module

Connecting the SCSI module to the Falcon can be performed in just a few steps:

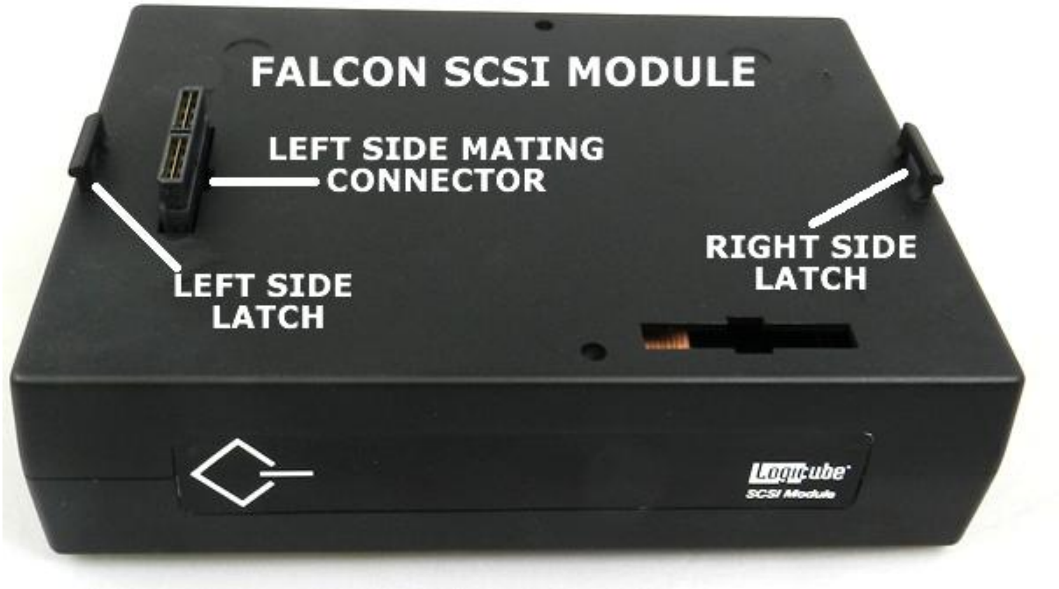
1. Turn the Falcon upside-down and locate the expansion cover to the right of the sticker.



2. Insert a small, sturdy tool (for example, an eyeglass screwdriver) as seen below. Pry the expansion cover off as shown below.



3. Carefully align the Falcon over the SCSI module. With the left side slightly lower (about a 15 degree angle) connect the left side latch of the SCSI module to the left side of the Falcon and align the left side mating connector to the open expansion slot on the Falcon. Next, slowly lower the right side and connect the right side latch to the Falcon.

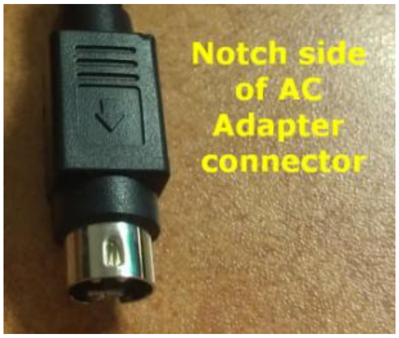


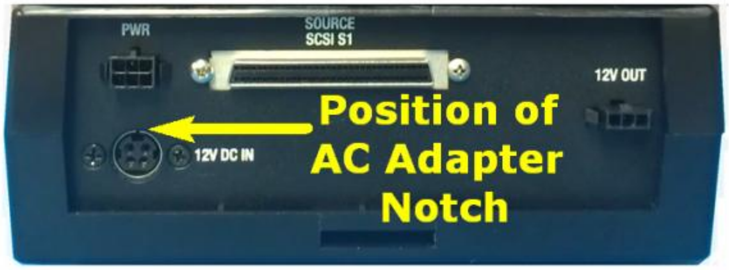
4. While holding the Falcon with SCSI module together, carefully turn the entire unit (Falcon and SCSI module) upside down. Insert the two 2.5” screws on each front and back side and tighten the screws so the Falcon unit and SCSI module are securely connected.

13.2 Turning the Falcon with SCSI module on and off

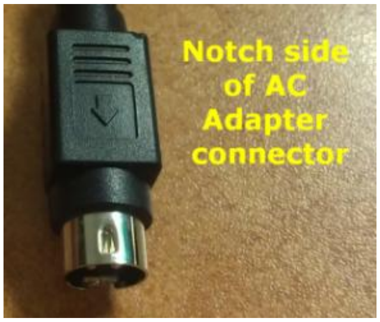
The Falcon and SCSI module each come with a 12V, 12.5A (output DC) power supply that connects to each device.

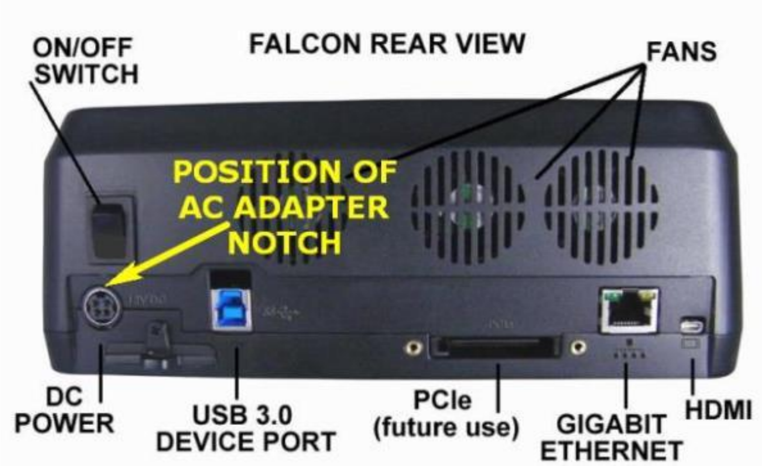
Attach one of the included power supplies to the left side of the SCSI module. The power supply has a ‘notch’ to guide the connection. The notch should be guided to face the top side of the power port.





Attach the other included power supply to the Falcon's power port in the back of the Falcon. The power supply has a 'notch' to guide the connection. The notch should be guided to face the top side of the power port.





When using both the Falcon and SCSI module, it is important to connect both power supplies to the Falcon and SCSI module before turning the Falcon's momentary switch on.

To turn the Falcon on, press and immediately release the top of the momentary on/off switch in the back. The Falcon will turn on and you should hear the fans turn on and see the display show the Falcon logo.

It is normal for the fans to either turn off or slow down after the initial start-up sequence.

There are two ways of turning the Falcon off:

1. Press and immediately release the top of the momentary on/off switch in the back. The Falcon will begin its shut down process and after a few seconds, the display and fans will turn off.
2. Using the Graphical User Interface (GUI) either on the touch screen or via a browser through a remote connection, navigate to the ***Power Off*** screen and tap or click the ***Power Off*** icon.

Once the power is completely off (GUI turns off along with the fans), it is safe to disconnect the power supplies from both the Falcon and SCSI modules.

13.3 Connecting Drives

This section shows how to connect SCSI drives to the Falcon's SCSI module. For information on how to connect other types of drives directly to the Falcon and not through the SCSI module, please see ***Section 2.2: Connecting Various Drive Types***.

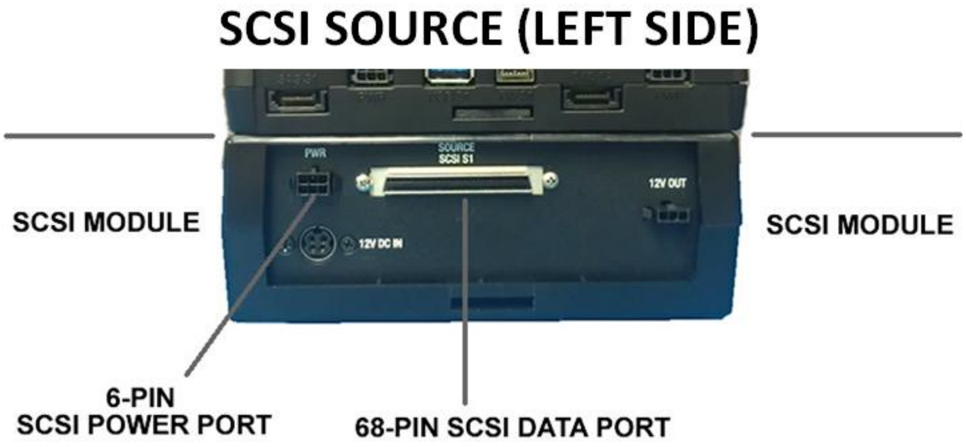
13.3.1 Connecting SCSI Source and Destination Drives

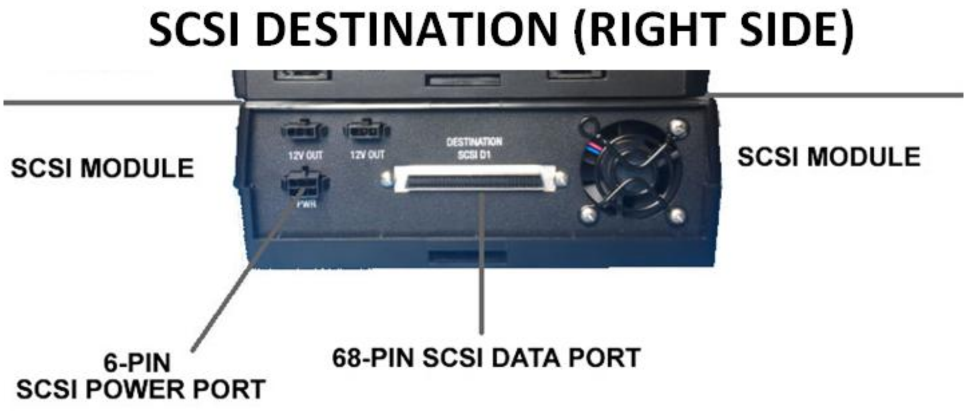
SCSI Source drives must be connected to the left side of the SCSI module. SCSI Destination drives must be connected to the right side of the SCSI module.

Two cables are required to connect one standard 68-pin SCSI drive:

- 68-pin data cable
- Drive power cable (CBL-EXT-PWR-04)

Simply connect the two cables to the SCSI module and connect the other side of the cables to the SCSI drive.





50-pin and 80-pin adapters are available. Please contact Logicube Sales to purchase these adapters.

For 50-pin drives, connect the 50-pin adapter between the 68-pin data cable and the drive. To power 50-pin drives, connect the drive power cable directly to the drive.

For 80-pin drives, connect the 80-pin adapter between the 68-pin data cable and the 80-pin drive. To power 80-pin drives, connect the drive power cable to the 80-pin adapter. The 80-pin drive has a Single Connector Attachment (SCA) which provides the transmission of both data and power.

14: Forensic USB Boot Client

14.0 Introduction

A Forensic Falcon USB (iSCSI) Boot Client (Forensic bootable USB flash drive for use with the Falcon) is available. The bootable flash drive allows the imaging of a Source drive from a computer on the same network without booting the native Operating System on the computer and can be imaged without having to remove the drive from the computer.

Details on how to create the forensic USB boot client can be found on the Forensic Falcon's support page at http://www.logicube.com/knowledge/forensic-falcon.

15: FREQUENTLY ASKED QUESTIONS

15.0 FAQs

Q. Why is it when I image a drive the number of bytes shown is twice the size of my Source drive?
A. The number of bytes shown on the progress bar is not the actual size of the drive. This is the actual data being processed. When 'Verify' is set to "Yes", the reported number will double in size.

Q. Is there a way to image a drive inside a computer without having to remove it and connect it directly to the Falcon?
A. Yes. There is a Forensic USB Boot Client for the Falcon. The Application Note and Instructions can be found on the Falcon support page: http://www.logicube.com/knowledge/forensic-falcon

Q. How many concurrent tasks can the Falcon run?
A. The Falcon can run up to 5 concurrent tasks.

Q. Do Destination drives need to be wiped or formatted using the Falcon?
A. Logicube recommends using the Falcon to wipe or format Destination drives. The Falcon logs all wipe and format operations.

Q. Can the Falcon image Linux partitions?
A. Yes. Falcon can image Linux partitions.

Q. Can the Falcon image a Hierarchical File System (HFS)?
A. Yes, Falcon can image HFS.

Q. How does the Falcon handle bad sectors found on the Source drive?
A. Falcon will retry the bad sector 7 times. After the 7th attempt, if the sector still cannot be read, it will skip that sector and list the sector in the log file.

Q. What operating system does Falcon use?
A. Falcon uses a Linux-based operating system. A Linux-based operating system provides increased stability and security over Windows-based systems.

Q. What file format does Falcon use when formatting destination drives?
A. Falcon can format destination drives using the NT File System (NTFS) or EXT4 file system.

Q. Does imaging performance slow down when multiple drives are imaged at the same time?
A. Performance is limited by the slowest drive in the configuration, however, there should not be any significant speed penalty when imaging multiple drives.

Q. How many separate tasks can you have running concurrently?

A. You can have up to five separate tasks running concurrently.

Q. Can I schedule or automate tasks?

A. Falcon features the ability to create up to 5 separate “Tasks Macros”. Each macro allows you to set up to 9 operations to be performed sequentially. For example, if your routine procedure is to wipe a drive before you begin imaging, then image a drive using e01 mode (S1 to D1), then hash (S1), you can add these operations to a Macro and from the Falcon GUI select the Macro and the Falcon will perform the specified tasks/operations in the sequence you have defined. The user can save the Macro to use in future imaging sessions. Administrators can set up Macros to provide an easier method for novice users or first responders to image suspect drives in the field.

Q. Can I encrypt my evidence drives using the Falcon? How do I decrypt drives encrypted with Falcon?

A. The Falcon provides AES 256 whole drive encryption. Users can choose between three different cipher modes and can set their own password/key for the encrypted drive. Users can decrypt a drive that was encrypted with Falcon by using the Falcon to decrypt or by using TrueCrypt or FreeOTFE.

Q. Can the Falcon image to or from a network destination?

A. Yes. The Falcon includes a gigabit network connection. Users can designate a network share as a source or destination repository using CIFS (Common Internet File System) or iSCSI (Internet Small Computer System Interface) protocols.

Q. What is “Parallel Imaging”?

A. Parallel Imaging allows you to image from the same source drive to multiple destinations using different formats, image to a network location using e01, image to one destination drive using dd format, and image to a 2nd destination drive using native (mirror format). This is useful when there are multiple teams of investigators (one in a lab and one at another location but connected to a network) and you also need to provide a copy of the suspect hard drive to those that require an exact mirror image (for example to an attorney).

Q. What is a “filter-based file copy”?

A. In many cases, investigators want to image only specific file types on a suspect’s hard drive, this can be useful to shorten the imaging process. The Falcon’s “file” mode allows users to specify by extension type e.g. .jpeg, .pdf, .mov, .xls etc. which files they want to image. The files will be sorted by path (based on where the file is located on the Source). If a hash method is selected, each file will be hashed.

Q. Does the Falcon provide log files?

A. Yes, each operation/task produces a log file. The log file is viewable on the Falcon screen (or remotely on a PC) in an HTML format. The log files can be exported to a thumb drive (the Falcon will export in XML, HTML and PDF). XML log files can be customized using XML editors. The log files are stored on the internal hard drive within Falcon and are accessible by pressing the log file icon from the left-side navigation bar on the Falcon screen.

Q. Can I remove the internal hard drive for secure locations or SCIFs?

A. Often investigators must work in a sensitive compartmentalized information facility (SCIF). These secure areas have very stringent requirements regarding the use of electronic devices to ensure sensitive information does not leave the confines of the SCIF. The Falcon has been designed with a removable internal hard drive. The Falcon’s operating system, system settings and log files are all stored on this internal drive. If an investigation requires that the Falcon must be removed from the SCIF or be transported to another location, the internal drive can be removed prior to leaving the facility. It is a good practice to always make a back-up copy of the hard drive prior to entering a secure location.

Q. If I am imaging to or from USB enclosures, will the Falcon's USB ports power my devices or will an additional power source be required?
A. Each of the Falcon's USB ports meets the standard specification of up to 5V of power. If your USB device has higher power requirements an external power source will be necessary. Check with the manufacturer of your USB device to determine the exact power requirements.

Q. Can the Falcon image to an external storage device such as a NAS (Network Attached Storage)?
A. Yes, Falcon can image to external storage devices. The external device can be connected to Falcon via the Gigabit Ethernet or via the destination ports (USB 3.0 or the SAS/SATA) built into Falcon. If the external storage device has a RAID configuration it will require that it be configured as a single drive. Any source drive connected to Falcon can be imaged directly to the external storage device.

16: Index

Technical Support Information

For further assistance please contact
Logicube Technical Support at: **(001) 818 700 8488 7am-5pm PST, M-F (excluding US legal holidays)**
or by email to **techsupport@logicube.com**

Software Attribution

Ubuntu 12.04 LTS (http://www.ubuntu.com)
Linux Kernel (3.2.48) (GPL v2) (http://www.kernel.org) (modified)
libcli (1.9.5) (LGPL v2.1) (https://github.com/dparrish/libcli) (modified)
monitorix (3.2.1) (GPL v2) (http://www.monitorix.org) (modified)